

Open Source at a Crossroads: A Call to Action

This report is designed as a resource for members of the Open Source community, providing a foundational overview of the critical challenges currently facing open source operating systems and software. While it aims to be comprehensive, it is intended as a starting point for dialogue and strategic discussion, not as a definitive or exhaustive guide. Some information herein may not be immediately actionable but is offered to inform, educate, and provide necessary context.

The ultimate goal is to spark conversation and inspire coordinated efforts **to safeguard open source operating systems and software from being regulated out of existence** in the United States or otherwise pushed out of the marketplace.

While I hope to update this document as circumstances evolve, my ability to do so is limited by ongoing personal issues. For this reason, I encourage others to freely build upon this work—anyone may take this report, adapt it, expand upon it, or revise it as they see fit.

A Note on Sources and Scope: I am not an academic researcher, and I cannot guarantee that every citation or reference meets formal scholarly standards. However, I have made a genuine effort to ensure accuracy and proper attribution throughout. ***Beyond just documenting sources, this report also seeks to raise awareness of certain issues and intersectional concepts that may not have been widely considered before.*** If you identify any errors, see an opportunity to expand on these ideas, or have thoughts on how to improve the work, please feel free to either revise the document directly or reach out to me by email.

Transparency Note: This report was drafted with the assistance of DeepSeek AI, a generative artificial intelligence tool, which helped refine and structure the content based on my direction and input.

Sam Treviño

Please report any issues with this report to sam@whyurban.com.

Age Assurance Laws and the End of General Purpose Computing

California AB 1043, Colorado SB 26-051, KOSA, and the EU's Parallel Path

Open Source Elimination, Trillion-Dollar Market Transfer, and the Hardware Attestation Endgame

Prepared: March 5, 2026

Executive Summary

A coordinated multi-level regulatory strategy is now entrenched at both state and federal levels, fundamentally reshaping the relationship between citizens, their devices, and the state. California's AB 1043 (Digital Age Assurance Act) takes effect January 1, 2027, requiring operating system level age attestation. Colorado's SB 26 051, modeled on California's approach, follows on January 1, 2028. Texas, Utah, and Louisiana have laws already operative as of 2026 (Loeb & Loeb LLP, 2025). However, the enforcement of the Texas App Store Accountability Act (SB 2420) was preliminarily enjoined by a federal court in late 2025 on grounds that it likely violates the First Amendment and is impermissibly vague (Fox Rothschild LLP, 2026). At the federal level, 19 new digital media bills are under consideration, including a revised Kids Online Safety Act (KOSA) and COPPA 2.0, marking what Davis Wright Tremaine LLP (2026) describes as a "wave of federal 'online safety' legislation" poised to fundamentally reshape the internet.

Critically, these new laws do not operate in a vacuum. They build upon and interact with the existing federal Children's Online Privacy Protection Rule (COPPA), which was significantly strengthened by amendments effective April 22, 2026 (Federal Trade Commission, 2026a). The state laws' age signal mechanisms trigger COPPA's "actual knowledge" standard (Loeb & Loeb LLP, 2025), forcing app developers who receive age information to comply with COPPA's detailed requirements, including written security programs, data retention policies, and verifiable parental consent (Federal Trade Commission, 2026a; 16 CFR §§ 312.5, 312.8(b), 312.10). The **FTC (Federal Trade Commission)** has explicitly endorsed this convergence, issuing a February 2026 policy statement encouraging age verification technologies while warning that information collected must be used solely for verification and promptly deleted (Federal Trade Commission, 2026b).

This report analyzes these state laws, pending federal legislation, and COPPA's foundational role, examining their interplay, their combined impact on open source software, and the deeper structural concerns raised by critical examination, particularly regarding the potential for mission creep toward mandatory digital identification, hardware attestation, and comprehensive surveillance infrastructure that would render Fourth Amendment protections meaningless. The **EU (European Union)** is pursuing parallel policies, confirming a global convergence toward OS-level age verification and the technological building blocks for hardware-enforced compliance (FOSDEM, 2026; SPIRS Project, n.d.).

Recent developments indicate that what was once a warning is now an entrenched reality. Open source communities are actively discussing compliance or geoblocking (Nestor, 2026; James, 2026; Dawe, 2026). Google and Apple have launched age verification APIs (Loeb & Loeb LLP, 2025). The bipartisan consensus that once propelled these laws is splintering amid constitutional concerns and industry influence (Lima-Strong, 2025). Research from the National Science Foundation reveals that **FTC (Federal Trade Commission)** enforcement is so under-resourced that developers fear app store removal more than government action, a dynamic the state laws exploit by leveraging platform power (Egelman, 2023).

Beyond the immediate compliance burden lies a deeper structural transformation: the systematic exclusion of open source operating systems and software from the market, effectuated through regulatory design rather than direct prohibition. When projects like MidnightBSD announce they will "exclude California from desktop use entirely" (Nestor, 2026), they are not merely protecting themselves from liability—they are ceding their user base in the nation's most populous state to corporate alternatives. This market transfer mechanism serves convergent government and corporate interests: governments gain universal surveillance infrastructure, while corporations gain monopoly pricing power freed from the downward pressure that free open source alternatives previously exerted. A 2024 Harvard-backed study estimates the demand-side value of the open source ecosystem at approximately **\$8.8 trillion**, with companies needing to spend 3.5 times more on software if open source did not exist (Open Source Initiative, 2026). The stakes of this market transfer are thus measured in trillions of dollars.

The endgame, already visible in federal studies and international developments, is **hardware-level attestation** that would fundamentally alter this dynamic. Under such a regime, new computing devices would cryptographically validate that the operating system and software are certified compliant before allowing the system to boot or connect to networks. This would render open source operating systems impossible to run on any new

device sold in the United States, regardless of user sophistication, and close the loophole of practical impunity that currently protects open source users. The EU is simultaneously funding hardware root of trust research through its Horizon 2020 program, indicating global convergence toward hardware-enforced compliance (SPIRS Project, n.d.).

Part I: The Entrenched National Landscape of Age Assurance Legislation

1.1 Operational State Laws

As of March 2026, multiple state laws are already in effect or scheduled to take effect imminently, fundamentally altering the compliance landscape for operating systems and applications (Loeb & Loeb LLP, 2025).

State	Law	Effective Date	Status
Texas	App Store Accountability Act	January 1, 2026	Enjoined pending litigation (Fox Rothschild LLP., 2026)
Utah	App Store Accountability Act	May 7, 2026	Partially effective
Louisiana	App Store Accountability Act	July 1, 2026	Effective
California	AB 1043 (Digital Age Assurance Act)	January 1, 2027	Signed into law
Colorado	SB 26 051 (Age Attestation for Online Users Act)	January 1, 2028	Pending
Alabama	App Store Accountability Act	2026	Enacted (Loeb & Loeb LLP, 2025)

Table 1

According to Loeb & Loeb LLP (2025), several other states across the country, including Florida, New York and Ohio, introduced age verification legislation in 2025. The law firm notes that "app store laws made the jump from state to federal when Sen. Mike Lee, R-Utah, and Rep. John James, R-Mich., introduced the App Store Accountability Act, a federal version similar to the state laws that would preempt those state laws."

1.2 States with Proposed "Age Signal" Legislation

State	Bill	Type	Status
Illinois	HB 3304 / HB 4140	Digital Age Assurance Act (Age Signal)	Proposed
New Hampshire	(Not specified)	Age Signal Model	Proposed

Table 2

1.3 Age-Appropriate Design Code States

State	Law	Status
California	Age-Appropriate Design Code	Enjoined
Maryland	Age-Appropriate Design Code	Challenged
Nebraska	Age-Appropriate Design Code	Enacted
Vermont	Age-Appropriate Design Code	Enacted
South Carolina	Age-Appropriate Design Code	Pending

Table 3

1.4 California's AB 1043: The Template

California's Digital Age Assurance Act (AB 1043), signed by Governor Gavin Newsom in October 2025, takes effect January 1, 2027. According to James (2026) at Tom's Hardware, the law's broad definition of an "operating system provider" encompasses anyone who "develops, licenses, or controls the operating system software on a computer, mobile device, or any other general purpose computing device" pulling in not just Windows, macOS, Android, and iOS, but Linux distributions and Valve's SteamOS.

Key Requirements:

- Operating system providers must provide interface at account setup for age declaration
- Age converted to non-identifiable age bracket signal ("under 13," "13 15," "16 17," "18+")
- Developers must request signal when app downloaded and launched
- Developers deemed to have "actual knowledge" of user's age upon receiving signal
- No parental consent required for downloads; no verification (self-declaration only)
- Enforcement by Attorney General only (no private right of action)

Assemblymember Buffy Wicks, who authored the bill, stated that this approach "avoids constitutional concerns by focusing strictly on age assurance, not content moderation" (James, 2026). The bill passed both chambers unanimously, 76 0 in the Assembly and 38 0 in the Senate.

However, James (2026) reports that despite signing it, Newsom issued a statement urging the legislature to amend the law before its effective date, citing concerns from streaming services and game developers about "complexities such as multi- user accounts shared by a family member and user profiles utilized across multiple devices."

1.5 Colorado's SB 26-051

Colorado's SB 26 051, modeled closely on California's approach, creates a mandatory age attestation system built into operating systems with substantially similar requirements, effective January 1, 2028. The bill defines "User" as a minor who is the *primary user* of a device, creating significant practical problems for shared family devices.

1.6 Texas, Utah, and Louisiana: The "Commercially Reasonable" Model

These states take a different approach, requiring app stores to verify age using "commercially reasonable methods" (potentially IDs, credit cards, biometrics). Key characteristics include:

- Requires parental consent for each app download
- Links minor accounts to parent accounts
- Significant changes to apps trigger renewed parental consent

The Texas law has been preliminarily enjoined on First Amendment grounds, suggesting this model faces significant legal hurdles (Loeb & Loeb LLP, 2025).

1.7 Federal Legislation: 19 Bills Under Consideration

According to Davis Wright Tremaine LLP (2026), the U.S. House of Representatives' Subcommittee on Commerce, Manufacturing, and Trade recently held a hearing on 19 new federal digital media bills, including:

Bill	Key Provisions
Kids Online Safety Act (KOSA)	Duty of care, safeguards for minors, parental tools, transparency reports
COPPA 2.0	Raises coverage to under 17, prohibits targeted advertising, "eraser button" (in consultation with HHS - U.S. Department of Health and Human Services)
App Store Accountability Act	Federal version of state laws requiring age verification at app store level
RESET Act	Prohibits minors under 16 from maintaining social media accounts
Sammy's Law	Requires API access for third party safety software
SPY Kids Act	Restricts market research on minors
Safer GAMING Act	Requires protective features for minors in online video games
SCREEN Act	Age verification to prevent minors from accessing sexually explicit content; requires GAO (Government Accountability Office) report on effectiveness
SAFE BOTs Act	Requires disclosures about chatbots and limits on compulsive use
SMK Act	Bars ephemeral messaging for minors, mandates parental controls

Table 4

1.8 The Unraveling Bipartisan Consensus

Lima-Strong (2025) reports that the once-surging alliance of federal lawmakers pushing to bolster protections for children online is splintering. At a December 2, 2025 hearing of the House Energy and Commerce Committee, key Democratic lawmakers hammered the panel's Republican leaders for diluting protections in KOSA and COPPA 2.0.

Rep. Lori Trahan (D- MA) stated that "the flagship proposals for today's hearing ... have been gutted and co- opted by Big Tech, and in their process of backroom deal- making, committee leadership has shunned parents, advocates and bipartisanship" (Lima-Strong, 2025).

Rep. Kathy Castor (D- FL) said Republicans are now pushing ahead with "weak, ineffectual versions" that amount to a "gift to the Big Tech companies" and a "slap in the face" to those seeking strong guardrails (Lima-Strong, 2025).

The latest House version of KOSA removes the core "duty of care" standard present in earlier iterations, instead requiring companies to submit to annual audits and maintain "reasonable policies" to address harms like violence and sexual abuse (Lima-Strong, 2025).

1.9 Constitutional Concerns

Davis Wright Tremaine LLP (2026) notes that several of the federal proposals raise constitutional concerns. While the Supreme Court upheld a Texas law requiring age verification to access adult content in *Free Speech Coalition, Inc. v. Paxton*, 606 U.S. 461 (2025), laws restricting or conditioning access to fully protected speech, presumptively banning minors from broad swaths of the internet, or imposing design and duty-of-care mandates on speech intermediaries have consistently failed First Amendment scrutiny.

At the December 2025 hearing, House Energy and Commerce Chairman Brett Guthrie defended the measures, stating that the bills were "curated to withstand constitutional challenges," adding, "A law that gets struck down protects no one, and if that happened, we'd fail to protect the very children we're here to protect" (Lima-Strong, 2025).

1.10 The Hardware Attestation Pathway

KOSA Sec. 107 requires a study of "device or operating system level age verification systems," including "technical feasibility, including the need for potential hardware and software changes" (Kids Online Safety Act, S. 1748, 119th Cong. § 107, 2025). The FTC's February 2026 policy statement endorses "one-time, centralized age verification" that can be "portable and used across different platforms" (Federal Trade Commission, 2026b). These provisions, combined with state OS mandates, create a clear pathway toward hardware attestation requirements that would fundamentally alter the relationship between users and their devices.

1.11 Key Trends and Observations

Three Tiered Approach: The regulatory landscape now has three distinct but overlapping models: state level "commercially reasonable" verification (Texas, Utah, Louisiana), state level "age signal" OS mandates (California, Colorado, Illinois), and federal platform regulation (KOSA).

Constitutional Challenges: The Texas law has been preliminarily enjoined on First Amendment grounds, suggesting the "commercially reasonable" approach faces significant legal hurdles. KOSA's duty of care provision faces similar vulnerabilities.

Federal State Interplay: KOSA explicitly permits states to provide greater protection, meaning California's and Colorado's OS mandates continue in effect. Platforms must comply with both federal platform requirements and state OS requirements.

Privacy Paradox: The California/Colorado "age signal" model claims to be privacy preserving through self-declaration and data minimization, while KOSA claims privacy protection through its prohibition on affirmative age collection. Yet both create infrastructure that can be repurposed for surveillance.

Hardware Pathway: Current laws and studies are constructing the on-ramp to hardware-level attestation, which would make open source operating systems impossible to run on new devices.

1.12 The Preemption Uncertainty

It remains unclear whether federal legislation will preempt these state laws or coexist with them. The House versions of both KOSA and COPPA 2.0 include preemption language that could override stronger state protections, while the Senate versions do not contain such provisions (American Action Forum, 2025; Fight for the Future, 2025). This distinction has drawn sharp criticism from Democrats and state attorneys general, who warn that broad preemption would "wipe out existing state laws on the books that keep kids safe" (Broadband Breakfast, 2025). In February 2026, a bipartisan coalition of 40 attorneys general urged Congress to reject the House version and pass the Senate bill to preserve states' authority to enforce their own youth safety laws (WRGB, 2026). The App Store Accountability Act (H.R. 3149) also includes an explicit preemption section (Sec. 9), indicating that federal legislation in this area may displace state requirements. As of this writing, the outcome remains uncertain, with competing bills advancing through Congress and the preemption question hotly debated.

Part II: COPPA as the Invisible Partner

2.1 The Foundational Federal Framework

The Children's Online Privacy Protection Rule (COPPA), codified at 16 CFR Part 312, implements the Children's Online Privacy Protection Act of 1998. It imposes requirements on operators of websites and online services directed to children under 13, or operators with actual knowledge that they are collecting personal information from children (Federal

Trade Commission, 2026a). Significantly, COPPA was strengthened by amendments effective **April 22, 2026**, making it an increasingly potent partner to the new state laws.

2.2 Key 2025-2026 COPPA Amendments

Amendment	Previous Rule	New Rule (Effective April 22, 2026)	Significance
Personal Information Definition	Limited categories	Expanded to include biometric identifiers (fingerprints, facial patterns, DNA sequences, voiceprints) and government-issued identifiers (state IDs, birth certificates) (Federal Trade Commission, 2026a)	Regulatory creep as technology evolves; more data captured
Parental Consent	Single consent	Separate, additional verifiable consent required before disclosing children's data to third parties (Federal Trade Commission, 2026a)	Creates additional friction and data collection points
Data Retention	Vague guidance	Written data retention policy required; indefinite retention prohibited; must delete when no longer reasonably necessary (Federal Trade Commission, 2026a)	Formalizes surveillance infrastructure
Security Program	"Reasonable procedures"	Mandatory written information security program with designated coordinator, annual risk assessments, regular testing (Federal Trade Commission, 2026a)	Imposes corporate-style compliance burdens
Mixed Audience Sites	Unclear	Defined and required to age-gate before any collection (Federal Trade Commission, 2026a)	Forces age verification on more sites
Safe Harbor Programs	Minimal oversight	Must publicly disclose membership lists and report regularly to FTC (Federal Trade Commission, 2026a)	Increased transparency creates pressure

Table 5

2.3 The "Actual Knowledge" Trigger

The state laws' most significant impact is creating a pipeline through which app developers gain **actual knowledge** of users' ages via OS or app store APIs. Under COPPA § 312.2, an operator with "actual knowledge" that it is collecting personal information from a child under 13 must comply with all COPPA requirements (Federal Trade Commission, 2026a).

As Loeb & Loeb LLP (2025) warns: "If an app developer has actual knowledge that a child is under the age of 13 because the app store has given the app developer the child's age, the app developer will now have to comply with COPPA for that user, including deleting any personal information it had previously collected from the child."

The Creep Mechanism: State laws that merely require age signals effectively deputize COPPA as the enforcement mechanism. The developer cannot simply comply with the state law; they must now comply with the entire COPPA apparatus, including written security programs, data retention policies, and verifiable parental consent.

2.4 The FTC's February 2026 Policy Statement

On February 25, 2026, the FTC issued a landmark **Policy Statement on Age Verification** that fundamentally alters the relationship between COPPA and state laws (Federal Trade Commission, 2026b).

The Policy Statement provides:

"The Commission will not bring an enforcement action under the COPPA Rule against operators of general audience sites and services and mixed audience sites and services that collect, use, or disclose personal information for the sole purpose of determining a user's age without first obtaining verifiable parental consent—if they comply with certain **conditions**" (Federal Trade Commission, 2026b).

The Conditions:

1. Use information only for age verification
2. Delete information promptly after verification
3. Disclose only to third parties with reasonable security assurances
4. Provide clear notice to parents and children
5. Employ reasonable security safeguards
6. Take reasonable steps to ensure accuracy

The FTC explicitly acknowledged the "chicken-versus-egg dilemma" between age verification and COPPA compliance (Federal Trade Commission, 2026b). The policy statement is a direct response to state laws requiring age verification. As The National Law Review (2026) noted, the FTC's announcement "comes amid a flurry of hotly-debated—and often challenged in court—state laws that require websites to verify users' ages."

This is not coincidence. It is coordinated regulatory action.

2.5 The FTC Commissioner's Vision

FTC Commissioner Mark Meador stated at the January 2026 workshop that age verification is "not novel" and parallels age gates for cigarettes and alcohol (Federal Trade Commission, 2026b). He specifically commended the development of tools allowing for **"one-time, centralized age verification"** that can be **"portable and used across different platforms"** — a single age verification that follows the user everywhere. The **General Data Protection Regulation (GDPR)**, Europe's comprehensive privacy law, would govern how such systems could be implemented in the EU, imposing strict requirements on data collection, purpose limitation, and user rights.

This is exactly the infrastructure this report warned about.

2.6 The Mixed Audience Trap

The 2025 COPPA amendments define "mixed audience" sites as those directed to children but not primarily targeting them (Federal Trade Commission, 2026a). Such sites must:

- Age-gate before collecting any personal information
- Cannot collect information from any visitor prior to age determination
- Must use neutral age collection methods that do not default to a set age

The Open Source Problem: Any open source project that might be used by children (which is virtually any project) could be deemed "mixed audience" under the expanded factors. The FTC will now consider marketing materials, representations to third parties, user reviews, and the age of users on similar services (Federal Trade Commission, 2026a). Open source projects have no control over user reviews or third-party representations.

2.7 The "Support for Internal Operations" Limitation

COPPA's definition of "support for the internal operations" (§ 312.2) allows certain activities without parental consent, but with a critical limitation:

"The information collected for these activities cannot be used or disclosed to contact a specific individual, including through behavioral advertising, **to amass a profile on a specific individual**, or for any other purpose" (Federal Trade Commission, 2026a).

This directly addresses the surveillance concern in the report. **However, this is a legal prohibition, not a technical one. The infrastructure built for age verification exists. The data exists. The legal limitation can be changed, ignored, or interpreted away. The report's surveillance thesis (Part VIII) addresses what the infrastructure *can* do; this section addresses what the law currently *prohibits*.** The tension is not between conflicting claims but between technical capability and legal restraint—a restraint that can be altered by future legislation, reinterpreted by courts, or circumvented by executive action.

Part III: State Law Mechanics and Regulatory Frameworks

3.1 Comparison of State Approaches

Aspect	California AB 1043	Colorado SB 26 051	Texas/Utah/Louisiana
Primary Target	Operating System Providers	Operating System Providers	App Stores
Core Mechanism	OS level age attestation + age signal API	OS level age attestation + age signal API	Commercially reasonable age verification
Age Collection	Mandatory at OS account setup	Mandatory at OS account setup	App store collects at account creation
Verification Method	Self-declaration	Self-declaration	IDs, credit cards, biometrics
Parental Consent	Not required	Not required	Required for each download/purchase
Age Brackets	Under 13, 13-15, 16-17, 18+	Under 13, 13-15, 16-17, 18+	Same four categories
Enforcement	Attorney General	Attorney General	Attorney General
Developer Knowledge	Deemed actual knowledge	Deemed actual knowledge	Required to comply with laws

Table 6

3.2 Age Bracket Definitions

All state laws apply the same age ranges and designations (Loeb & Loeb LLP, 2025):

- Younger than 13 = child
- 13 15 = younger teen
- 16 17 = older teen
- 18 and over = adult

3.3 API Integration Requirements

Both Google and Apple have announced the launch of new APIs that will allow apps to receive a user's age range and supervision status. Google launched the New Play API and Apple launched its Declared Age Range API. The app store accountability laws require app developers not only to incorporate these APIs but also to verify the age category of the users through these APIs (Loeb & Loeb LLP, 2025).

Importantly, all the state laws provide a safe harbor from certain violations if app developers have properly implemented these APIs and are using the age verification shared through them (Loeb & Loeb LLP, 2025).

3.4 Penalties

Violation Type	Penalty (per affected minor)
Negligent	Up to \$2,500
Intentional	Up to \$7,500

Table 7

Part IV: The KOSA Federal Framework

4.1 Key Provisions

Provision	Summary	Analysis
Covered Platform Definition	Online platforms, online video games, messaging applications, or video streaming services that connect to the internet and are used or reasonably likely to be used by a minor	Broad definition potentially covering many services
Duty of Care (Revised)	Platforms must maintain and enforce "reasonable policies" to prevent specified harms (Lima-Strong, 2025)	Weakened from earlier versions; the core "duty of care" standard has been removed in the latest House version, replaced by annual audit requirements and "reasonable policies" to address harms
Safeguards for Minors	Must provide safeguards limiting communications, protecting personal data, controlling recommendations, and restricting geolocation sharing; most protective default settings for minors	Mandates specific technical features
Parental Tools	Must provide tools for parents to manage privacy settings, restrict purchases, and view/limit time spent	Creates surveillance infrastructure within families
Reporting Mechanism	Readily accessible means to report harms; substantive response within 10 days (large platforms) or 21 days (small platforms)	Creates databases of reported incidents
Age Verification Study	Requires study of methods for verifying age at device or operating system level	Direct federal parallel to state experiments
Enforcement	FTC enforcement; State attorneys general may enforce	Dual enforcement mechanism
Preemption	Preempts state laws only to extent they conflict; permits states to provide greater protection	State laws like California's and Colorado's continue in effect

Table 8

Note on Legislative Status: The provisions described above reflect KOSA as introduced in the 119th Congress. However, as Lima-Strong (2025) reports, the latest House version has removed the core "duty of care" standard, replacing it with annual audit requirements and "reasonable policies" to address harms like violence and sexual abuse. This represents a significant weakening of the bill from earlier iterations.

4.2 COPPA 2.0 (HR 6291)

Davis Wright Tremaine LLP (2026) outlines key provisions of COPPA 2.0:

- Raises the age of coverage from under 13 to under 17
- Prohibits targeted advertising directed at children and teens
- Requires explicit consent from users aged 13 to 16 before collecting or processing personal information
- Introduces an "eraser button" requirement for parents and teens to delete personal information
- Establishes a dedicated Youth Marketing and Privacy Division within the FTC

4.3 Key Differences from State Approaches

Aspect	California/Colorado	KOSA
Primary Target	Operating System Providers	Online Platforms and Services
Core Mechanism	OS level age attestation + age signal API	Duty of care + safeguards + parental tools
Age Collection	Mandatory at OS account setup	Prohibited from requiring affirmative collection
Age Verification	Attestation only (self-declaration)	Not required; study ordered for future
Hardware Requirements	Requires OS modifications	None directly, but study may lead to future requirements
Enforcement	State Attorneys General	FTC and State Attorneys General
Open Source Impact	Directly targets operating systems	Targets platforms and services

Table 9

4.4 The Bernstein Framework: Tech Liability vs. Parent Gatekeeper

Legal scholar Gaia Bernstein provides a valuable theoretical framework for understanding the different regulatory approaches documented in this report. In a December 2025 article summarizing Bernstein's work, Sridhar (2025) distinguishes between the **Tech Liability Model**, which holds technology companies responsible for keeping children safe online, and the **Parent Gatekeeper Model**, which holds parents responsible.

Model	Description	Examples	Critique
Tech Liability Model	Holds technology companies responsible for keeping children safe online	KOSA's duty of care; risk assessment requirements; bans on addictive design features	Places responsibility on those who design harmful systems
Parent Gatekeeper Model	Holds parents responsible for children's online activity	Parental consent requirements; parental control tools	Permits tech companies to evade responsibility; raises privacy concerns

Table 10

The Tech Liability Model—exemplified by KOSA's duty of care provisions, risk assessment requirements, and bans on addictive design features—places responsibility on those who design and profit from systems that may harm children. The Parent Gatekeeper Model—exemplified by parental consent requirements and parental control tools—shifts responsibility to parents while allowing tech companies to continue operating without fundamental changes.

Sridhar (2025) notes that Bernstein argues the Parent Gatekeeper Model "permits technology companies to evade responsibility for harms children face as a result of excessive screen time—harms the industry caused to begin with" and that "parents are ineffective at protecting their children from online harms" due to the complexity of parental controls, the social pressure to allow children access to peer networks, and the inherent difficulty of constant monitoring. Bernstein further contends that the Parent Gatekeeper Model raises privacy concerns by granting parents access to children's online communications, while the Tech Liability Model better protects privacy by limiting data

collection (Sridhar, 2025). This framework provides theoretical support for the parenting critique advanced in Part X.

Part V: The Combined Regulatory Burden

5.1 Layered Compliance Requirements

Entities operating in the online ecosystem face compliance requirements at multiple levels:

Entity Type	State Requirements	Federal Requirements (Pending)	COPPA Requirements	Combined Effect
Operating System Provider	Must implement age attestation interface and API (California, Colorado)	App Store Accountability Act would impose similar requirements	Not directly covered unless they collect children's information	OS providers face multiple state regimes plus potential federal overlay
App Developer	Must request age signal from OS; comply with age rating requirements; integrate Google/Apple APIs (Loeb & Loeb LLP, 2025)	KOSA, COPPA 2.0, and other bills impose additional duties	Once age signal received, COPPA applies to under-13 users, triggering written security programs, data retention policies, parental consent mechanisms	App developers face triple compliance: state OS level, federal platform level, and COPPA
Platform Operator	Must receive age signals from OS for users	Must implement all KOSA requirements	Must comply with COPPA for any under-13 users	Full compliance with all three regimes
Open Source Project	Cannot comply with OS mandate (no entity); effectively barred	Cannot comply with platform requirements (no resources); effectively barred	Cannot comply with COPPA's detailed requirements (impossible without corporate structure); effectively barred	Eliminated from US market entirely

Table 11

5.2 The Compliance To Do List

Loeb & Loeb LLP (2025) provides a compliance to- do list for app developers that illustrates the burden:

- Reassess your app's age category and update it on the app stores
- Integrate the Google and Apple APIs
- Develop and implement processes for handling minor users identified through the APIs
- Silo any information collected from the APIs for age verification purposes only
- Establish processes for when parents revoke previously given consent
- Establish processes for notifying app stores of material changes
- Determine whether your app must comply with COPPA or state privacy laws
- Determine whether the app can still collect personal information under applicable laws

This list assumes a corporate entity with legal counsel and engineering resources. For a community open source project, it represents an impossible burden.

5.3 The COPPA Compliance Checklist for Open Source

COPPA Requirement	Citation	Corporate Implementation	Open Source Project Reality
Written information security program	§ 312.8(b)	Legal counsel + security team	No resources to draft or maintain
Designated security coordinator	§ 312.8(b)(1)	Paid employee	Volunteer with other priorities
Annual risk assessments	§ 312.8(b)(2)	External or internal auditors	Impossible without funding
Regular testing of safeguards	§ 312.8(b)(4)	Dedicated security staff	No capacity
Third-party assurances	§ 312.8(c)	Contractual relationships	No legal entity to contract
Written data retention policy	§ 312.10	Legal drafting	No guidance available
Deletion when no longer necessary	§ 312.10	Automated systems	Manual impossible at scale
Separate consent for third-party disclosure	§ 312.5(a)(2)	Integration with payment/ID systems	Technically impossible
Parental access rights	§ 312.6	Support team infrastructure	No staff to handle requests
Verifiable parental consent methods	§ 312.5(b)	Credit card, government ID, knowledge-based authentication	Impossible without payment systems or ID verification
Mixed audience site compliance	§ 312.2	Age-gating before collection	Impossible without infrastructure

Table 12

5.4 The Compliance Cost Barrier and Unfunded Obligation

Cost Factor	Corporate Entity	Community Open Source Project	Verified Estimate Source
State Legal Review (Multiple regimes)	In house counsel or retained firms	\$1,000-\$3,400+/hour for specialized regulatory counsel; unaffordable	(ABA Journal, 2026; ResearchAndMarkets.com , 2025)
Federal Legal Review (KOSA, COPPA 2.0, etc.)	In house counsel or retained firms	\$1,000-\$3,400+/hour for specialized regulatory counsel; unaffordable	(ABA Journal, 2026; ResearchAndMarkets.com , 2025)
COPPA Legal Review	In house counsel or retained firms	\$1,000-\$3,400+/hour for specialized regulatory counsel; unaffordable	(ABA Journal, 2026; ResearchAndMarkets.com , 2025)
OS Implementation (California/Colorado)	Existing engineering teams	Volunteer effort; impossible without paid staff	(Report analysis)
API Integration (Google/Apples APIs)	Dedicated engineering resources	Volunteer effort; technically complex	(Report analysis)
COPPA Security Program	Security team + legal	Impossible without dedicated staff	(Report analysis)
Platform Safeguards (KOSA requirements)	Product and engineering teams	New development; impossible without resources	(Report analysis)
Parental Tools (KOSA requirements)	Product teams	Impossible without data collection infrastructure	(Report analysis)
Reporting Mechanism (KOSA requirements)	Support and trust/safety teams	Impossible to staff at scale	(Report analysis)
Third Party Audits (KOSA requirements)	Third-party audits for KOSA-like compliance frameworks typically cost \$10,000–\$100,000+, depending on organizational scope and complexity	Impossible; no budget	(Good, 2025)
Liability Insurance	Bundled corporate coverage (\$500-\$2,000+/year for general liability or BOP)	Unattainable for volunteers (no legal entity, no revenue, no insurable business operations)	(Homebase, 2024; U.S. Small Business Administration, 2024)

Table 13

Note on Insurance Accessibility: According to Homebase (2024), most small businesses pay approximately **\$500 to \$2,000** a year for general liability insurance or a Business Owner's Policy (BOP), with general liability typically running **\$40 to \$100** per month. The U.S. Small Business Administration (2024) notes that liability insurance premiums "vary widely among insurance companies, and depend on a number of risk factors, including your business location, building type, local fire protection services, and the amount of insurance you purchase." Insurance companies underwrite policies based on formal business entities with documented operations and revenue history. For volunteer open source projects, which lack legal entities, revenue streams, and traditional business operations, commercial liability insurance is structurally unattainable regardless of cost.

This creates an **unfunded obligation** that disproportionately harms open source projects at every level. As defined in this report, an unfunded obligation in the context of an open source project occurs when outside parties such as corporations, government bodies, or a broad user community anticipate, insist on, or mandate specific updates, security reviews, upkeep, or regulatory adherence, yet fail to supply the necessary financial support, staffing, or development effort to make those expectations a reality. This definition is original to this report and is used throughout to describe the structural mismatch between regulatory expectations and open source project capabilities.

Unlike corporations, which can pass compliance costs onto customers or absorb them as cost of doing business, open source projects have no revenue stream, no legal entity to hold insurance, and no paid staff to implement mandated features. The obligation is therefore not just costly but structurally impossible to fulfill.

5.5 Open Source Outcomes by Project Type

The combined regulatory framework produces different outcomes for different categories of open source projects. These distinctions are critical to understanding the varied claims throughout this report:

Project Type	Examples	Likely Outcome	Explanation
US-Based Community Projects	Small Linux distros, independent FOSS projects	Eliminated or forced to geoblock	Cannot afford compliance; no legal entity; personal liability for developers
US-Based Corporate-Backed Projects	Ubuntu (Canonical), Fedora (Red Hat)	May survive through compliance investment	Corporate backing provides resources for legal review, implementation, and ongoing compliance
EU-Based Projects	Linux Mint, Debian, many European distros	Survive by serving US users remotely	Beyond US jurisdiction; can continue distributing to US users while developers remain protected by EU sovereignty
Hardware-Dependent Projects	Projects requiring new device sales	Eliminated from future US market	Hardware attestation will make them impossible to run on new US devices
Pre-Attestation Hardware Projects	Projects targeting older devices	May survive on existing hardware	Users who stockpile pre-2028 devices can continue running non-compliant software

Table 14

These outcomes explain the varied claims throughout the report: open source is eliminated from US market entirely for US-based community projects; cedes user base through geoblocking for projects that choose that path; becomes legally non-viable for projects without corporate backing; survives through EU structuring for European projects; becomes impossible to run on new US devices for projects affected by hardware attestation.

5.6 The MidnightBSD Precedent

According to Nestor (2026), some OS developers, like MidnightBSD, have decided to exclude California from desktop use entirely. This represents a form of geoblocking that may become more common as open source projects recognize the impossibility of compliance. Each such announcement transfers market share to corporate alternatives.

MidnightBSD has since drafted what an alternative implementation might look like, suggesting writing a user's age to a file readable by root only (Ridley, 2026). In the Google Doc for the potential change, developers noted the absurdity: "Would it be legal to ask if you want to turn this feature off and skip this crap outside the US?" (Ridley, 2026). The project also modified its license to exclude California residents, placing the burden of enforcement on state authorities. As PC Gamer observed, this means "the job of checking whether people have installed its OS falls onto Californian authorities to deal with. How might they go about that? Again, seems practically impossible, and boggles the mind to even suggest such a thing could occur" (Ridley, 2026).

5.7 Ubuntu's Unresolved Compliance Path

As of March 2026, Canonical has not announced a compliance path for Ubuntu under California's AB 1043. Jon Seager, VP Engineering at Canonical, stated that the company is "aware of the legislation and is reviewing it internally with legal counsel, but there are currently no concrete plans on how, or even whether, Ubuntu will change in response" (Nestor, 2026). Seager emphasized that recent mailing list discussions were "informal conversations among Ubuntu community members, not an announcement," and that none of the proposed ideas have been "adopted or committed to by Canonical" (Nestor, 2026).

This uncertainty, shared by Fedora and other distributions, reinforces the analysis in Section 9.1 and suggests that even corporate-backed distributions may struggle to implement compliant solutions before California's January 1, 2027 effective date.

Part VI: Market Transfer and the Privatization of Computing

6.1 The Market Share Dynamic

The compliance burden is not merely an existential threat to open source projects—it functions as a **market transfer mechanism**. When projects like MidnightBSD announce they will "exclude California from desktop use entirely" (Nestor, 2026), they are not simply protecting themselves from liability. They are **ceding their user base** in the nation's most populous state to corporate alternatives.

Traditional View	Market Transfer View
Compliance costs make open source impossible	Open source is <i>forced out of markets</i> by regulatory design
Open source dies	Open source's <i>market share</i> is transferred to corporate entities
Privacy is lost	Privacy becomes a <i>premium product</i> only available to those who can pay
Surveillance becomes possible	Surveillance becomes <i>inevitable</i> because all remaining options are corporate-controlled

Table 15

6.2 The Market Transfer Mechanism

Phase	Mechanism	Effect
1	State/federal laws impose compliance costs	Open source cannot afford; corporate can
2	Open source projects geoblock or shut down	Users lose access to open source options
3	Users migrate to corporate alternatives	Market share transfers to corporate entities
4	Corporate entities gain monopoly power	Prices can increase; surveillance infrastructure expands
5	Open source becomes niche or extinct	Privacy-respecting options eliminated

Table 16

When MidnightBSD excludes California users, those users will not stop needing operating systems. They will migrate to Windows, macOS, or corporate-backed Linux distributions (Ubuntu, Fedora, RHEL) that can afford compliance. Each geoblocking announcement transfers another segment of the user base to corporate control.

6.3 The Rising Costs Argument

Linux holds an estimated **5.03%** of the US desktop market (as of June 2025) and approximately **4.1%** globally (as of June 2025), with global share having reached an all-time high of 4.44% in July 2024 (Command Linux, 2025). Even at these modest percentages, Linux functions as a price ceiling. If Windows raised prices too high, more users would switch. If macOS became too expensive, users could buy cheaper hardware and run Linux. The existence of a viable free alternative constrains the entire market.

Before Open Source Exclusion:

OS Type	Price	Market Share (Worldwide, Jan 2026)	Market Share (United States, Jan 2026)	Pricing Pressure	Source
Windows	\$139.00 (Windows 11 Home download)	67.7%	61.5% (estimated from StatCounter)	Constrained by free alternatives	(Microsoft, 2026; StatCounter Global Stats, 2026a, 2026c)
macOS	Bundled with Apple hardware (\$1,099+ for MacBook Air)	11.79% (combined)	18.4% (estimated from StatCounter)	Constrained by upgrade cycle	(Buzzi, 2026; StatCounter Global Stats, 2026a, 2026c)
Linux (various)	\$0	4.1%	5.03% (from June 2025)	Provides ceiling on pricing	(Devuan GNU+Linux, 2025; Command Linux, 2025)
Unknown/Other	—	15.26%	14.1% (estimated from StatCounter)	—	(StatCounter Global Stats, 2026a, 2026c)

Table 17

Note: StatCounter's United States data includes an "Unknown" category (14.1% in January 2026) that represents operating systems not specifically identified in their tracking methodology. Windows and macOS figures are estimates based on the identifiable portion of the market. Due to variability in Linux market share data on the StatCounter Global Stats website, the more stable figures from Command Linux were cited instead.

After Open Source Exclusion:

OS Type	Price	Market Share	Pricing Pressure	Source
Windows	\$139.00+ (no constraint)	Growing	None	(Microsoft, 2026)
macOS	Bundled (no escape)	Growing	None	(Buzzi, 2026)
Linux	Geoblocked/unavailable	0%	Eliminated	(Report analysis)
ChromeOS	Possibly monetized	Captive	None	(Report analysis)

Table 18

The Result: With no free alternative, corporate OSes face no price competition. Prices will rise. Not immediately, perhaps, but over time as monopoly power consolidates. The 2-4% of users who would have switched to Linux are now captive.

6.4 The Consumer Harm Framework

The market transfer imposes multiple forms of harm on consumers:

Type of Harm	Description	Manifestation
Price Harm	Consumers pay more	Corporate OS prices rise without free competition
Quality Harm	Consumers get less	Privacy-invasive features cannot be avoided
Choice Harm	Consumers have fewer options	Only corporate-controlled OSes available
Innovation Harm	Less innovation	Corporate inertia, no community experimentation

Table 19

6.5 The MidnightBSD Precedent as Market Transfer

Nestor's (2026) report that "MidnightBSD, have decided to exclude California from desktop use entirely" is not an isolated incident. It is a case study in the market transfer mechanism:

1. **Regulatory Imposition:** California AB 1043 requires OS-level age attestation. Compliance cost: prohibitive for small projects.
2. **Project Response:** MidnightBSD announces it will exclude California users. This is framed as liability protection.

3. **User Migration:** California users who want a desktop OS must choose Windows, macOS, or corporate-backed Linux distributions.
4. **Market Transfer Complete:** California users lose access to a privacy-respecting, community-developed OS. Corporate market share grows.

6.6 The Trillion-Dollar Stake

The Open Source Initiative (2026) reports that a Harvard-backed study estimates the demand-side value of the open source ecosystem at approximately **\$8.8 trillion**, with companies needing to spend 3.5 times more on software if open source did not exist (Open Source Initiative, 2026). This figure places the market transfer mechanism in stark economic perspective: the elimination of open source represents not merely a loss of user autonomy and privacy, but the forced migration of nearly nine trillion dollars in value from community-developed infrastructure to corporate-controlled alternatives. The regulatory framework described in this report is not just reshaping the software market—it is orchestrating one of the largest wealth transfers in economic history.

Part VII: The Unified Theory of Coordinated Market Capture

7.1 The Core Thesis

A coherent and structurally sound theory explains the observed phenomena more completely than any alternative: state and federal governments are cooperating with corporations to push open source operating systems and software out of the market. This cooperation serves mutual interests:

Party	Benefit
Governments	Surveillance and control infrastructure becomes universal and unavoidable
Corporations	Market monopoly achieved; pricing power obtained; open source's downward price pressure eliminated

Table 20

The cooperation need not be explicit conspiracy. It can be convergent interests pursued through parallel action, with industry lobbying shaping legislation and agencies implementing rules that favor corporate compliance while making community models impossible.

7.2 What Governments Gain

Government Interest	How Open Source Blocks It	How Corporate Control Enables It
Surveillance	Open source can be audited; tracking can be removed; phone-home features can be disabled	Corporate OSES have mandatory telemetry; data flows to corporate servers; government can access via legal process
Control	Open source can be modified; users control their own experience; updates can be declined	Corporate OSES enforce updates; features cannot be removed; user autonomy eliminated
Law Enforcement Access	Open source has no corporate parent to subpoena; data may not exist to seize	Corporate entities respond to warrants, NSLs, FISA orders; data is collected by default
Regulatory Compliance	Open source cannot be compelled; no entity to fine; distributed development resists pressure	Corporations have assets, employees, and presence; they can be regulated, fined, and compelled
National Security	Foreign contributors cannot be vetted; code cannot be controlled	Corporate code can be audited (in theory); single point of control exists

Table 21

7.3 What Corporations Gain

Corporate Interest	How Open Source Blocks It	How Regulatory Exclusion Enables It
Market Monopoly	Open source provides free alternatives; users can leave	Open source eliminated; users are captive
Pricing Power	Free software exerts downward pressure on prices	No free alternatives; prices can rise
Data Monetization	Open source typically doesn't collect or sell user data	All users generate data; all data can be monetized
User Lock-In	Open source can be modified; users control their experience	Corporate OSES control updates, features, terms
Competitive Pressure	Open source innovation forces corporate adaptation	Corporate inertia; innovation on corporate terms
Liability Avoidance	Open source has no entity to sue; corporations bear liability	Liability exists but can be managed; costs passed to consumers

Table 22

7.4 The Symbiotic Relationship

The arrangement is mutually reinforcing:

Government Needs Surveillable Platforms



Government Creates Regulatory Barriers



Corporations Help Design the Regulations



Regulations Favor Corporate Compliance Models



Open Source Cannot Comply; Is Forced Out



Users Migrate to Corporate Platforms



Corporations Gain Market Share and Data



Governments Gain Access to Data and Users



Loop Reinforces: More Surveillance, More Control

7.5 The Surveillance Synergy

The surveillance dimension reinforces the pricing dynamic. Under the corporate model, consumers pay monetary costs *and* surrender privacy. The data collected is then monetized, generating additional revenue that could theoretically lower prices, but in practice increases corporate profits while consumers bear both burdens.

Factor	Open Source	Corporate OS
Data Collection	None by default; user can audit	Mandatory telemetry; cannot disable
Data Value	None	Monetized to offset costs
Government Access	None (no data to access)	Routine via legal process
User Cost	Free (monetary) + privacy preserved	Paid (monetary) + privacy surrendered

Table 23

7.6 The "Tax on Freedom" Quantified

The elimination of open source imposes costs on every user, whether they ever used open source or not, because it removes the competitive constraint that kept corporate prices and surveillance in check.

Cost Type	Under Open Source	Under Corporate Monopoly
Monetary Cost	\$0	\$100-\$500+ per device
Privacy Cost	\$0 (privacy preserved)	Immeasurable (surveillance)
Autonomy Cost	\$0 (user controls device)	Immeasurable (device controls user)
Choice Cost	\$0 (multiple options)	Immeasurable (no alternatives)
Innovation Cost	\$0 (community innovation)	Immeasurable (corporate inertia)

Table 24

7.7 The Irony of "Protection" Complete

The full irony of the "protection" framing is now visible:

Framing	Reality
"Protecting children online"	Eliminating privacy-respecting options
"Protecting national security"	Creating universal surveillance infrastructure
"Protecting consumers"	Enabling monopoly pricing
"Protecting competition"	Eliminating competitors
"Protecting privacy"	Mandating data collection

Table 25

7.8 Regulatory Capture as Explanatory Framework

The patterns documented throughout this report—industry-friendly compliance standards, exclusion of non-corporate actors, convergence of government and corporate interests—are consistent with the theory of **regulatory capture**. First articulated by economist George Stigler, regulatory capture occurs when regulatory agencies, through close contact with the industries they oversee, come to act in the interests of those industries rather than the public.

In the context of age assurance legislation, regulatory capture manifests in several ways:

- **Industry drafting:** Corporate lobbyists participate directly in bill drafting
- **Revolving doors:** Regulators and legislators move between government and industry positions
- **Information asymmetry:** Agencies rely on industry expertise to understand technical implications
- **Compliance design:** Requirements are structured around corporate capabilities
- **Exclusionary effects:** Costs are calibrated to eliminate non-corporate competitors

As Stigler observed, regulation often serves not to protect the public but to create barriers to entry that benefit established firms. The elimination of open source from regulated markets, and the resulting transfer of market share to corporate entities, exemplifies this dynamic.

7.9 Public Choice Dynamics

The legislative outcomes described in this report are consistent with public choice theory, which analyzes how self-interest shapes political decision-making. Key insights include:

- **Concentrated benefits, diffuse costs:** The benefits of excluding open source accrue to a small number of corporate entities with strong incentives to lobby; the costs are spread across millions of users who face privacy loss, higher prices, and reduced choice—making organized opposition difficult.
- **Rational ignorance:** Voters have little incentive to understand complex regulatory issues; legislators face correspondingly little electoral pressure to resist industry lobbying.
- **Rent-seeking:** Corporations invest in shaping regulation to capture economic rents (monopoly profits) rather than in productive competition.

These dynamics explain why legislation that harms consumers and eliminates competition can nonetheless attract bipartisan support: the benefits are concentrated and well-funded; the opposition is diffuse and poorly organized.

Part VIII: The Antitrust Paradox

8.1 The Government Action Defense

The arrangement described in Part VII would be illegal if done by corporations alone. Traditional antitrust law prohibits monopolization, predatory pricing, exclusive dealing, and conspiracies in restraint of trade under Sections 1 and 2 of the Sherman Act (15 U.S.C. §§ 1-2). Yet this coordinated exclusion of open source from the market is not an antitrust violation because **government action is exempt** under the state action doctrine first recognized in *Parker v. Brown*, 317 U.S. 341 (1943). The Supreme Court held that the Sherman Act was not intended to "nullify a state's control over its officers and agents" and that "an unexpressed purpose to nullify a state's control over its officers and agents is not lightly to be attributed to Congress" (*Parker v. Brown*, 1943, p. 351).

For private conduct to qualify for this exemption, the Supreme Court established a two-part test in *California Retail Liquor Dealers Ass'n v. Midcal Aluminum*, 445 U.S. 97, 105 (1980): (1) the challenged restraint must be "one clearly articulated and affirmatively expressed as state policy," and (2) the policy must be "actively supervised by the State itself." When municipalities act pursuant to a clearly articulated state policy, they need not meet the "active supervision" prong if the anticompetitive conduct is a "foreseeable result" of state authorization (*Town of Hallie v. City of Eau Claire*, 1985).

Antitrust Violation	Description	This Scenario	Legal Basis
Predatory Pricing	Selling below cost to drive out competitors	Not applicable (open source is free)	15 U.S.C. § 2
Exclusive Dealing	Contracts that exclude competitors	Regulatory compliance as exclusive dealing	15 U.S.C. § 1
Monopolization	Willful acquisition of monopoly power	Government-facilitated monopoly	15 U.S.C. § 2
Conspiracy in Restraint of Trade	Agreement to restrain competition	Convergent interests achieve same result	15 U.S.C. § 1

Table 26

8.2 The Antitrust Paradox

Element	Traditional Antitrust Violation	This Scenario	Legal Basis
Actor	Dominant firm	Government (at corporate urging)	<i>Parker v. Brown</i> , 317 U.S. 341 (1943)
Mechanism	Predatory pricing	Regulatory compliance costs	15 U.S.C. § 2
Target	Competitors	Open source projects	15 U.S.C. §§ 1-2
Effect	Monopoly achieved	Corporate control achieved	(<i>Town of Hallie v. City of Eau Claire</i> , 1985).
Legality	Illegal	Legal (because government did it)	State Action Doctrine

Table 27

8.3 The Irony of Antitrust Enforcement

There is a deep irony in this dynamic, particularly in light of the Sherman Act's purpose "to protect the public against the evils of monopoly" (*Parker v. Brown*, 317 U.S. at 351):

- **The same government agencies** (FTC, DOJ) that enforce the Sherman Act (15 U.S.C. §§ 1-2) are participating in creating these regulatory moats
- **The same legislators** who decry Big Tech monopoly power are voting for laws that will entrench Big Tech monopoly power
- **The same arguments** used against monopolists (lack of choice, rising prices, consumer harm) will be validated by the very laws passed in the name of "protection," yet those laws will be immune from antitrust challenge under the state action doctrine

8.4 Regulatory Moats

The concept of **regulatory moats** describes barriers to entry created not by market efficiency but by regulation.

Moat Type	Description	Example	Antitrust Status
Natural Moat	Intrinsic market advantages	Network effects, economies of scale	Not regulated
Corporate-Created Moat	Anticompetitive conduct	Predatory pricing, exclusive deals	Prohibited under 15 U.S.C. §§ 1-2
Regulatory Moat	Government-created barriers	Licensing, compliance costs, certification	Immune under <i>Parker v. Brown</i> (1943)

Table 28

What the combined state and federal framework creates is a regulatory moat around the operating system market, with open source as the primary target for exclusion. Corporations benefit from this moat without having to engage in conduct that would violate the Sherman Act (15 U.S.C. §§ 1-2), because the barriers are created by government action that is exempt from antitrust scrutiny under the state action doctrine. *Parker v. Brown*, 317 U.S. at 351.

8.5 European Privacy Standards as a Constraint

The French data protection authority (**CNIL** - Commission Nationale de l'Informatique et des Libertés) has provided a crucial precedent for how privacy-preserving age verification must operate. In July 2025, the CNIL ruled that augmented cameras using AI to estimate age for tobacco and alcohol sales violate GDPR principles of necessity and proportionality (Commission Nationale de l'Informatique et des Libertés, 2025).

The CNIL's reasoning directly supports the privacy concerns raised throughout this report: "These algorithmic age estimation devices inherently present risks to the fundamental rights and freedoms of individuals" (Commission Nationale de l'Informatique et des Libertés, 2025). The authority warned that the technology's design "involves default and continuous activation... leading to filming all people" and "prevents individuals from exercising their right to object" (Commission Nationale de l'Informatique et des Libertés, 2025).

This ruling establishes that any age verification system deployed in Europe must be narrowly tailored, avoid indiscriminate surveillance, and preserve individuals' ability to exercise their rights. It provides a benchmark against which US age assurance laws—particularly those that require OS-level data collection from all users—will be measured, and suggests that European courts may strike down systems that fail to meet these standards.

8.6 Human Rights Framework

Beyond US constitutional protections, the age assurance framework implicates international human rights law. Article 12 of the Universal Declaration of Human Rights provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence." Article 17 of the International Covenant on Civil and Political Rights (ICCPR) contains nearly identical language.

The UN Human Rights Committee has interpreted these provisions to require that:

- Collection of personal information be limited to what is necessary
- Data be protected against unauthorized access or misuse

- Individuals have rights to access and correct their data
- Independent oversight of surveillance activities exist

Hardware attestation that blocks uncertified operating systems may also implicate rights to freedom of expression (access to information) and freedom of association (ability to communicate using chosen tools). The European Convention on Human Rights Article 8 has been interpreted by the European Court of Human Rights to protect against indiscriminate surveillance and data retention—principles that could be invoked against US laws that mandate data collection and enable government access.

Part IX: Open Source Community Response

9.1 Ubuntu's Cautious Approach

According to Nestor (2026) at 9to5Linux, Ubuntu developer Aaron Rainbolt recently proposed on the Ubuntu mailing list an optional **D-Bus** (an inter-process communication system that allows software applications to communicate with each other) interface (org.freedesktop.AgeVerification1) that could be implemented by arbitrary applications as a distribution sees fit. However, Canonical responded that the company does not yet have a solution to announce.

Jon Seager, VP Engineering at Canonical, stated: "Canonical is aware of the legislation and is reviewing it internally with legal counsel, but there are currently no concrete plans on how, or even whether, Ubuntu will change in response. The recent mailing list post is an informal conversation among Ubuntu community members, not an announcement. While the discussion contains potentially useful ideas, none have been adopted or committed to by Canonical" (Nestor, 2026).

9.2 Community Discussions Across Distributions

Nestor (2026) reports that similar talks are underway in the Fedora and Linux Mint communities about implementing similar features in upcoming releases of their distributions to address the California law. At the same time, other OS developers, like MidnightBSD, have decided to exclude California from desktop use entirely.

Jef Spaleta, Fedora Project Leader, elaborated further on Fedora's approach, suggesting that age information may need to be tied to account creation and stored in a file accessible to applications (Dawe, 2026). Spaleta proposed that "this might be as simple as extending how we currently map uid to usernames and group membership and having a new file in /etc/ that keeps up with age," which could be populated through administrative tools at

account creation (Dawe, 2026). He emphasized that this would require "no telemetry... just a way for applications to query the OS... a local API... sounds a lot like a dbus service to me" (Dawe, 2026). This approach, if implemented, would create a standardized mechanism across Linux distributions while minimizing data collection.

The law applies to all GNU/Linux distributions, desktop environments, and application hubs like Flathub or Snap Store, which will have to comply in some way (Nestor, 2026).

9.3 The Global Context

Nestor (2026) notes that this is becoming a global standard, not just in California or the United States, as the Digital Services Act (DSA) is already in full effect across the EU as of February 2024 to ensure privacy, safety, and security for minors.

9.4 The Enforcement Reality for Linux Distributions

James (2026) observes that enforcement against Linux distributions is likely to be problematic. DistroS like Arch, Ubuntu, Debian, and Gentoo have no centralized account infrastructure, with users downloading ISOs from mirrors worldwide, and can modify source code freely. These small distributions lack legal teams or resources to implement the required API. James (2026) suggests that a more realistic outcome for non-compliant distros is a disclaimer that the software is not intended for use in California.

9.5 The MidnightBSD Precedent

Nestor's (2026) report that "MidnightBSD, have decided to exclude California from desktop use entirely" represents a form of geoblocking that may become more common as open source projects recognize the impossibility of compliance. Each such announcement transfers market share to corporate alternatives.

9.6 Organized Policy Response

The open source community is organizing a coordinated policy response to the regulatory challenges documented in this report. The Open Source Initiative (**OSI**) has expanded its public policy work, hiring full-time policy managers in both the US and Europe to "educate policymakers about the benefits of open source software, track policy developments, and ultimately ensure that open source developers can continue doing their work" (Open Source Initiative, 2026).

OSI's Katie Steen-James observes that "policy can inadvertently restrict Open Source by imposing obligations that don't align with Open Source licensing or development models" (Open Source Initiative, 2026). The organization leads the Open Policy Alliance, "a coalition of nonprofit organizations that want to engage in U.S. policy discussions around Open

Source," intentionally lowering barriers for under-resourced communities to participate (Open Source Initiative, 2026).

This organized response complements the individual resistance strategies discussed in Section 12.5 and the legal defense frameworks in Section 12.6. It represents a recognition that open source must engage proactively with policy rather than simply react to legislation after enactment.

9.7 F-Droid's Legal Resilience Model

The F-Droid project, a free and open source Android app repository, has launched a legal resilience initiative with support from the Open Technology Fund's FOSS Sustainability Fund (F-Droid, 2025). The project's goals directly address the liability concerns raised throughout this report:

- "Shield individual contributors from legal liability and overreach"
- "Handle abusive legal threats in a consistent, safe, and efficient way"
- "Mitigate risk by improving our infrastructure, governance, and policies" (F-Droid, 2025)

Operating under the legal umbrella of The Commons Conservancy, a Netherlands-based nonprofit foundation, F-Droid has conducted in-depth interviews with legal experts from organizations including the Software Freedom Conservancy, Software Freedom Law Center India, Free Software Foundation Europe, Electronic Frontier Foundation, and Mozilla (F-Droid, 2025). The project is documenting its findings in a public blog series to help other FOSS projects navigate similar challenges.

This initiative provides a concrete model for the organized legal defense framework proposed in Section 12.6 and demonstrates that open source projects are actively preparing for the regulatory battles ahead.

9.8 The DB48x Precedent: Resistance Beyond Operating Systems

The resistance to age assurance laws extends beyond operating systems to unexpected software categories. The DB48x calculator project, which aims to rebuild and improve upon the "legendary" HP48 family of calculators and RPL programming language, added a legal notice to its documentation stating:

"As a consequence of recent legislative activity in [California] and [Colorado]:

- California residents may no longer use DB48x after Jan 1st, 2027.
- Colorado residents may no longer use DB48x after Jan 1st, 2028.

DB48x is probably an operating system under these laws. However, it does not, cannot and will not implement age verification" (Ridley, 2026).

As PC Gamer noted, "You know you've messed up when you've angered the math lot" (Ridley, 2026). This example illustrates the law's potentially absurd reach: a calculator project—software running on specialized hardware with no user accounts, no data collection, and no connection to the problems the laws purport to address—must either implement age verification or block entire states. The DB48x response mirrors MidnightBSD's approach: geoblocking as the only viable alternative to impossible compliance.

This example, while seemingly niche, illustrates a fundamental critique shared by many in the technical community. As Raindog308 (2026), a systems administrator and writer, argued, the California law represents "absolute insanity" because it was drafted without any apparent understanding of how software is actually built and distributed. The author highlighted gaping technical questions the statute fails to answer, such as how it could apply to "servers and other CLI-only installs, how to handle VMs, [and] whether the law is even applicable if the primary user is over 18" (Raindog308, 2026). The DB48x project's predicament is not an isolated anomaly, but a logical consequence of a law that fundamentally misunderstands the computing environments it purports to regulate.

Part X: The Parenting Question

10.1 Government as Substitute Parent

A fundamental critique of both state laws and federal proposals is that they represent **government stepping in to do what parents should be doing**. This combined regulatory framework codifies the presumption that parents are either unwilling or unable to supervise their children's online activities, necessitating state intervention through technological mandates.

Traditional Parental Responsibility	California/Colorado Replacement	KOSA Replacement
Monitoring child's online activity	OS level age tracking	Platform level parental tools
Discussing online safety with children	Automated content restrictions	Duty of care design
Making decisions about appropriate apps	Age signals that bypass parental input	Default most protective settings
Teaching responsible digital citizenship	Compliance mandates that require no parenting	Reporting mechanisms that replace conversation

Table 29

10.2 The Perverse Incentive

By shifting responsibility from parents to operating systems and platforms, the combined framework creates a perverse incentive:

- **Parents are relieved** of the responsibility to actively parent their children's online activities
- **Government gains** new regulatory authority and data collection capabilities at both state and federal levels
- **Corporations gain** new compliance infrastructure that doubles as surveillance capability
- **Children lose** the benefit of parental guidance in favor of algorithmic enforcement
- **Society bears** the cost of yet another expansion of regulatory power

10.3 The Absurdity of Technological Parenting

Both state laws and federal proposals presume that technology can replace parenting. California and Colorado presume a one-time age entry at account setup can parent a child throughout the life of a device. KOSA presumes platform design features can prevent complex psychological harms. Both ignore:

- Children grow older (the age entered at setup becomes increasingly inaccurate)
- Parenting is contextual and situational, not binary
- Parental involvement cannot be replaced by an API call or a duty of care

As this report contends, the combined regulatory framework represents a fundamental shift in the relationship between family and state: **this is effectively parents not parenting their kids so the government comes in for the safety of children to do what parents should be doing.**

10.4 The California Critique

The Reason Foundation has suggested modifying California's model to make age signaling **optional for parents** rather than compulsory, preserving privacy benefits while strengthening family agency (Reason Foundation, 2026). The commentary notes that AB 1043's privacy-preserving model is preferable to "commercially reasonable" approaches that incentivize collection of "driver's licenses, passports, or credit cards," and cites recent data breaches—including the Tea app breach exposing over 70,000 ID images and the Discord breach tied to UK age verification—as cautionary examples of what mandatory

verification can create (Reason Foundation, 2026). The Foundation argues that "true digital literacy depends on ongoing dialogue, trust, and continuous education about online risks, not on technical filters alone," and proposes that "an opt-in structure would preserve AB 1043's privacy benefits while strengthening family agency" (Reason Foundation, 2026). Neither California's nor Colorado's bills contain such an opt out provision, and federal proposals similarly mandate parental tools without addressing whether parents want or need them.

Part XI: The National Security Argument and the TikTok Precedent

11.1 The TikTok Template

The controversy surrounding TikTok before Congress provides a crucial template for understanding how "protection" arguments can be weaponized to justify control over software platforms. The **Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACAA)**, enacted in April 2024 as Division H of the supplemental appropriations act (P.L. 118-50), required ByteDance, Ltd. to divest TikTok's U.S. operations or face a nationwide ban on the application's distribution and maintenance in the United States (Protecting Americans from Foreign Adversary Controlled Applications Act, 2024; Benson, Brannon, & Lampe, 2024). The Act expressly defined "foreign adversary controlled application" to include applications operated by ByteDance, Ltd. and TikTok, set an effective date of 180 days after enactment, and provided an exemption only for "qualified divestitures" executed before the prohibition took effect (Protecting Americans from Foreign Adversary Controlled Applications Act, 2024, §§ 2(a)(2)(A), 2(c)(1), 2(g)(3)(A)). Senators Blackburn and Blumenthal, lead sponsors of KOSA, were prominent voices in the TikTok hearings. The Supreme Court unanimously upheld PAFACAA on January 17, 2025, in *TikTok Inc. v. Garland*, applying intermediate scrutiny and giving "substantial respect" to Congress's national security judgments (TikTok Inc. v. Garland, 2025; National Association of Attorneys General, 2025).

The core arguments made during the TikTok hearings map directly onto state laws and federal proposals:

Argument	Application to TikTok	Application to California/Colorado	Application to KOSA
Foreign Government Access	Chinese government could access American user data	"Foreign adversaries could contribute code to Linux distributions"	"Foreign owned platforms could harm American children"
Algorithmic Manipulation	TikTok's algorithm could influence public opinion	"Untrusted code could contain hidden manipulation"	"Recommendation systems must be controlled and transparent"
Lack of Transparency	US regulators cannot audit TikTok's operations	"Open source code can be modified after review"	Platforms must undergo third party audits
National Security Threat	TikTok presents an unacceptable risk	"Uncontrolled software presents an unacceptable risk"	"Unregulated platforms present an unacceptable risk"

Table 30

11.1.1 The PAFACAA Template

The PAFACAA framework provides a template for how similar logic could be applied to open source software. The Act contains several key features that parallel arguments increasingly deployed against community-developed software:

Feature	PAFACAA Implementation	Potential Application to Open Source
Targeting by Name/Source	The Act expressly defined "foreign adversary controlled application" to include applications operated by ByteDance, Ltd. and TikTok (Protecting Americans from Foreign Adversary Controlled Applications Act, 2024, § 2(g)(3)(A); Benson, Brannon, & Lampe, 2024).	Open source projects could be designated based on contributor geography or perceived foreign influence.
Structural Separation Requirement	The Act required a "qualified divestiture" as the only path to compliance, meaning ByteDance had to sever both control and any operational relationship with TikTok (Protecting Americans from Foreign Adversary Controlled Applications Act, 2024, § 2(c)(1); TikTok Inc. v. Garland, 2025).	Open source projects could be required to incorporate or transfer assets to US-controlled entities.
Severe Penalties	Noncompliance carries civil penalties of \$5,000 per user accessed , exposing companies like Apple, Google, Oracle, and Akamai to potential liabilities in the hundreds of billions of dollars (Protecting Americans from Foreign Adversary Controlled Applications Act, 2024; Rozenshtein, 2025; Anderson P.C., 2025).	Similar per-user penalties could be applied to platforms distributing open source software or to developers themselves.
Platform-Based Enforcement	The Act targets not the application itself, but the "app stores and internet hosting services" that enable its distribution (Protecting Americans from Foreign Adversary Controlled Applications Act, 2024; National Association of Attorneys General, 2025).	Enforcement against open source would similarly target hosting platforms (GitHub, SourceForge) and package managers.
Judicial Deference	The Supreme Court unanimously upheld PAFACAA in <i>TikTok Inc. v. Garland</i> (January 17, 2025), applying intermediate scrutiny and giving "substantial respect" to legislative judgments about national security (TikTok Inc. v. Garland, 2025; National Association of Attorneys General, 2025).	Courts would likely defer to similar national security claims about open source software.

Table 31

As Rozenshtein (2025) observes, the stakes for companies that continued providing services to TikTok after the statutory deadline were "nearly a trillion dollars in potential liability." The Supreme Court's unanimous decision affirmed that "preventing China from collecting vast amounts of sensitive data" constitutes an important governmental interest sufficient to justify substantial burdens on speech and commerce (TikTok Inc. v. Garland, 2025).

This creates the template for the report's argument that similar logic could be applied to open source software: labeling it as a national security threat, requiring corporate restructuring or certification, and using enforcement against platforms (app stores, hosting services, package repositories) rather than end-users. The Act's success in targeting a specific company by name, requiring structural separation, imposing severe penalties, and surviving constitutional scrutiny demonstrates the viability of this regulatory approach.

11.2 The Logical Extension to Open Source

If the TikTok logic is accepted, it naturally extends to open source software:

TikTok Argument	Open Source Parallel
"We cannot trust software controlled by a foreign adversary."	"We cannot trust software developed by unknown persons globally."
"The Chinese government could compel ByteDance to hand over data."	"Any government could compel a contributor to insert vulnerabilities."
"We need visibility into who controls the code."	"We need verified identities for all code contributors."
"The only safe solution is American ownership."	"The only safe solution is corporate controlled, audited software."

Table 32

11.3 The National Security Argument Against Open Source

The same logic that led to TikTok's forced divestiture is being deployed against open source software through state OS mandates and federal platform requirements:

The "Foreign Adversary Contribution" Theory

- Open source projects accept contributions from developers worldwide
- A hostile nation state could submit code introducing vulnerabilities or backdoors
- The distributed, volunteer nature of open source makes comprehensive auditing impossible
- Therefore, open source software cannot be trusted for critical applications

The "Supply Chain Attack" Framework

- The 2020 SolarWinds attack demonstrated how trusted software can be compromised
- Open source dependencies create massive attack surfaces
- Without centralized control and liability, open source presents unacceptable national security risks

The "Attribution" Problem

- If something goes wrong with proprietary software, there is a company to hold accountable
- If something goes wrong with open source, there is no one to blame
- National security requires clear lines of responsibility

11.4 The Privatization Solution

The logical policy response to this framing is the **forced privatization of open source software**. The combined state federal approach accelerates this progression:

Step	California/Colorado Mechanism	KOSA Mechanism	COPPA Mechanism	Combined Effect
1	OS level mandate requires entity to implement	Platform requirements require entity to comply	Security program requires entity to maintain	Open source projects need legal entities
2	Compliance costs impossible for volunteers	Audit and reporting costs impossible for volunteers	Annual risk assessments impossible without funding	Economic pressure toward corporatization
3	Age signal API requires ongoing maintenance	Duty of care requires ongoing assessment	Data retention policy requires legal drafting	Only corporations can sustain
4	Liability for non-compliance	Liability for design features	FTC enforcement authority	Personal liability for volunteers
5	Effectively bans community open source OS	Effectively bans community open source platforms	Effectively bans any project with US users	All open source becomes legally non-viable

Table 33

11.5 The Irony: Open Source as Security

Notably, national security arguments against open source ignore that open source software is often **more secure** than proprietary alternatives because:

- Code is visible to anyone who wants to audit it
- Problems can be fixed by anyone, not just employees
- No single point of failure or control

As cybersecurity expert Bruce Schneier has noted: "A bad system design is secure as long as the details remain secret, but quickly breaks once they are released. A good system design is secure even if the details are public" (Schneier, 2002, p. 344).

The push to eliminate open source in the name of national security therefore eliminates one of the most effective security models available.

11.6 The Congressional Failure to Address Root Causes

The Public Knowledge analysis of the TikTok legislation made a crucial observation: "Picking a single company to blame may make for good headlines, but it is not a substitute for comprehensive technology policy" (Collins, 2026). Congress missed an opportunity to:

What Congress Could Have Done	What Congress Did Instead
Create baseline privacy rules for all companies	Targeted a single app with a ban or divest mandate
Strengthen transparency across all platforms	Created political bargaining over one company's fate
Advance competition and interoperability measures	Handed sweeping discretion to the executive branch
Build expert oversight mechanisms	Produced a politically brokered ownership structure

Table 34

This same dynamic applies to both state and federal child safety legislation: targeting specific mechanisms (OS level age attestation, platform duty of care) without addressing the underlying issues of parental responsibility, privacy protection, or the unique characteristics of open source software.

Part XII: The Surveillance Imperative

12.1 The Open Source Community's Concern

The open- source community has erupted in criticism over risks like apps inferring exact birth dates or enabling government surveillance, which Nestor (2026) describes as "a profound and dangerous step toward a society in which anonymity in public life becomes a relic of the past."

12.2 API Data Restrictions

All three state laws coming into effect in 2026 prohibit the use of the information shared through the APIs for any purpose other than age verification, and the Texas law requires app developers to delete the information upon completion of any age verification processes. App developers must therefore have an established process for siloing any data obtained through the APIs to ensure that it is only used for age verification and deleted after it is used for that purpose (Loeb & Loeb LLP, 2025).

COPPA reinforces this requirement, mandating that personal information collected from children be retained only as long as reasonably necessary and then deleted (Federal Trade Commission, 2026a).

12.3 The Cooperation Framework

The infrastructure built for age assurance is equally usable for age surveillance. The data collected for compliance is equally usable for law enforcement. The corporate relationships established for certification are equally usable for warrantless data sharing.

Open source software, by its nature, resists this conflation. As James (2026) notes, Linux distributions have no centralized account infrastructure and users can modify source code freely. This transparency is fundamentally incompatible with mass surveillance. A computer running software that does not report to any corporate parent, that does not embed unique identifiers, that does not phone home with telemetry, is a computer that cannot be easily surveilled.

12.4 KOSA's Specific Surveillance Mechanisms

KOSA adds specific surveillance capabilities beyond state OS level data collection:

KOSA Provision	Surveillance Mechanism
Parental Tools	Parents gain access to minors' account settings, purchase history, and time spent metrics. This creates a pipeline for family level surveillance that platforms must enable.
Reporting Mechanism	Platforms must maintain databases of reported harms and respond substantively. These databases are accessible to law enforcement through cooperation provisions.
Audit Requirements	Third party auditors gain access to platform data and internal practices. Auditors may be compelled to disclose information.
Law Enforcement Cooperation	Preserves platforms' ability to cooperate with law enforcement and comply with legal inquiries.

Table 35

12.5 Civil Disobedience and Resistance Movements

The report's analysis of technical circumvention (Section 7.4) addresses individual evasion but does not consider organized civil disobedience as a potential response. Historical precedents include:

- **French resistance to Nazi occupation:** Individuals and networks concealed information and communication
- **Soviet samizdat:** Underground publishing networks distributed prohibited materials
- **Cypherpunk movement:** Organized resistance to government encryption controls

Resistance Form	Method	Legal Risk
Individual evasion	VPNs, alternative DNS	Low; no user liability
Organized distribution	Mirror networks, darknet hosting	Medium; potential facilitator liability
Civil disobedience	Public refusal to comply; educational campaigns	High; potential prosecution

Table 36

The elimination of open source may catalyze organized resistance, particularly among privacy advocates, technical communities, and civil liberties organizations. Such resistance could take the form of:

- Educational campaigns about circumvention methods
- Development and distribution of circumvention tools
- Public refusal to use certified operating systems
- Legal challenges and public awareness litigation

12.6 Organized Legal Defense

The report's recommendations (Section 13.1) mention supporting **EFF (Electronic Frontier Foundation)** , **ACLU (American Civil Liberties Union)** , and open source organizations but do not develop the concept of **organized legal defense** as a strategic response. Historical precedents include:

- **NAACP Legal Defense Fund:** Coordinated litigation strategy for civil rights
- **EFF's early work:** Defending hackers and supporting cryptography rights
- **ACLU's surveillance litigation:** Challenging government overreach

Organization	Focus	Relevance
EFF	Digital rights, surveillance, open source	Directly relevant
ACLU	Constitutional rights, privacy	First/Fourth Amendment challenges
Software Freedom Law Center	Open source legal support	Developer defense
EPIC (Electronic Privacy Information Center)	Privacy, surveillance	Policy advocacy

Table 37

These organizations could play several roles:

- **Pre-enforcement challenges:** Suing to block laws before enforcement
- **Developer defense:** Representing individual developers targeted by enforcement
- **Amicus briefs:** Supporting constitutional challenges
- **Public education:** Framing the issues for broader audiences

12.7 The SEP/FRAND Parallel

The age assurance certification regime bears comparison to the regulatory battles over **standard essential patents (SEPs)** and **FRAND (fair, reasonable, and non-discriminatory)** commitments. In both cases:

- Standardization creates gatekeepers
- Certification requirements can exclude competitors
- Access to the standard becomes essential for market participation
- Disputes arise over fair terms of access

SEP/FRAND Context	Age Assurance Context
Standard-setting organizations	Government certification authorities
Essential patents	Required certification
FRAND commitments	"Reasonable" access claims
Hold-up	Exclusion of open source
Royalty stacking	Cumulative compliance costs

Table 38

Open source advocates in the SEP context have argued that FRAND commitments should require royalty-free licensing for open source implementations. Similar arguments could be made in the age assurance context: if government mandates certification, it should be available to open source projects on non-discriminatory terms—including zero cost, given that open source projects have no revenue to fund certification fees.

12.8 The Carbon Tax Parallel

The report's concept of an "unfunded obligation" (Section 5.4) parallels debates about carbon taxes and regulatory cost externalization. In both cases:

- Regulations impose costs on certain actors
- Those costs can be shifted to others
- The question of who bears the burden is central to regulatory design

Carbon Tax Context	Age Assurance Context
Carbon emissions taxed	Compliance costs imposed
Costs passed to consumers	Costs borne by volunteers (cannot pass)
Regressive impacts	Disproportionate impact on small projects
Regulatory design choices	Exemptions for vulnerable actors
Just transition	Preservation of open source

Table 39

Just as carbon tax debates consider "just transition" provisions for workers and communities affected by decarbonization, age assurance debates should consider provisions that preserve open source as a public good. The current regulatory design externalizes costs onto volunteers who cannot bear them, effectively taxing the open source model out of existence.

12.9 The Legislative End Run

By making it law to require using corporate controlled operating systems and software that they can regulate, the government has accomplished through legislation what the Fourth Amendment was designed to prevent. The requirement is framed as consumer protection, child safety, or national security, but the effect is to ensure that every device in America runs software that can be surveilled.

The view that this is precisely the point cannot be dismissed. Open source operating systems and software represent a threat to the surveillance state not because they are insecure, but because they are uncontrollable. A computer running software that does not report to any corporate parent, that does not embed unique identifiers, that does not phone home with telemetry, is a computer that cannot be added to the national surveillance database.

The solution, from this perspective, is simple: make such computers illegal to use. Mandate that every device run software from entities that can be regulated, compelled, and cooperated with. Frame it as protection. Call it safety. And let the surveillance infrastructure grow naturally from the compliance requirements.

12.10 COPPA's Limitation and the Surveillance Gap

COPPA's definition of "support for the internal operations" (§ 312.2) explicitly prohibits using information collected for those purposes "to amass a profile on a specific individual" (Federal Trade Commission, 2026a). This is a legal prohibition, not a technical one. The infrastructure exists. The data exists. The legal limitation can be changed, ignored, or interpreted away.

12.11 Open Source as the Obstacle

The elimination of open source as a viable option on US devices is therefore not an unfortunate side effect of well-intentioned regulation but the logical outcome of a regulatory framework designed to ensure that all software is accountable, traceable, and controllable. And a system where all software is controllable is a system where all users are surveillable.

12.12 The Irony of "Protection"

The language of protection that surrounds both state laws and federal proposals serves to obscure what is actually being built. The infrastructure for age assurance is equally usable for age surveillance. The data collected for compliance is equally usable for law enforcement. The corporate relationships established for certification are equally usable for warrantless data sharing.

Open source software, by its nature, resists this conflation. It does not collect data by default. It does not embed tracking. It does not cooperate with surveillance because there is no corporate entity to compel cooperation. This is not a bug. It is the fundamental feature of software that is truly owned by its users.

The elimination of open source as a viable option on US devices is therefore not an unfortunate side effect of well-intentioned regulation. It is the logical outcome of a regulatory framework designed to ensure that all software is accountable, traceable, and controllable. And a system where all software is controllable is a system where all users are surveillable.

Part XIII: The Privatization Thesis

13.1 The Economic Squeeze Mechanism

The compliance costs documented in Sections 5.3 and 5.4 create an unfunded obligation that disproportionately harms open source projects. The progression follows a predictable pattern:

Phase	Mechanism	Effect on Open Source
1	Impose OS compliance costs (California/Colorado)	Small projects cannot afford
2	Impose platform compliance costs (KOSA)	Additional impossible burden
3	Impose COPPA compliance costs (security programs, data retention, parental consent)	Most detailed and expensive burden
4	Create liability risk	Volunteers unwilling to assume personal risk
5	Require insurance	Additional cost barrier
6	Demand ongoing updates	Maintenance burden increases
7	No entity, no compliance	Open source becomes legally non-viable

Table 40

13.2 Privatization Pathways

Pathway 1: Acquisition

- Compliance costs make independence impossible
- National security concerns make "uncontrolled" software politically unacceptable
- Projects seek corporate sponsors
- Corporations acquire projects
- Code moves from community to corporate control
- Government now has a single entity to regulate and compel cooperation for surveillance

Pathway 2: Dual Licensing

- Free version: Non-compliant, "illegal" in California and Colorado, unable to meet COPPA or KOSA requirements
- Paid version: Compliant, "safe," "trusted"
- Free version atrophies; project goes proprietary
- Government approves of "trusted" corporate versions that include surveillance capabilities

Pathway 3: Service Layer Mandate

- Local software becomes legally risky
- Users shift to cloud services
- Control moves from user to corporation
- Government can now surveil through corporate partnerships and data sharing agreements

Pathway 4: Geoblocking

- As MidnightBSD has done with California (Nestor, 2026), projects block US access entirely
- US users lose access to open source software
- Market share shifts to corporate alternatives

Pathway 5: Market Transfer

- Open source projects forced to geoblock or shut down due to compliance costs
- Users migrate to corporate alternatives
- Corporate market share increases
- Consumer costs rise
- Surveillance becomes universal
- Open source eliminated not by direct ban but by regulatory exclusion from markets

13.3 The Ideological Capture

The combined state federal framework redefines "responsible" software:

Traditional Open Source Value	California/Colorado's Implicit Value	KOSA's Implicit Value	COPPA's Implicit Value	Surveillance Outcome
Privacy (collect nothing)	Compliance (collect age data)	Compliance (enable parental tools)	Compliance (collect for verification)	Continuous data collection
User Control	OS Control	Platform Control	Corporate Control	No user modification possible
Transparency	Black Box API	Black Box Audits	Black Box Security	Code hidden, surveillance hidden
Anonymity	Verified Identity	Verified Age	Verified Identity for children	Every user identified

Table 41

Over time, software that doesn't collect user data becomes legally suspect. Software with anonymous contributors becomes a national security threat. Software that doesn't cooperate with surveillance becomes contraband.

Part XIV: The International Enforcement Problem

14.1 Jurisdictional Limits: The Linux Mint Case Study

James (2026) notes that enforcement against Linux distributions is likely to be problematic. Distros like Arch, Ubuntu, Debian, and Gentoo have no centralized account infrastructure, with users downloading ISOs from mirrors worldwide, and can modify source code freely. These small distributions lack legal teams or resources to implement the required API.

14.2 The "Minimum Contacts" Standard

For a foreign developer to be subject to US jurisdiction, they must have "purposefully directed" activities at the US:

Factor	Legal Weight	Linux Mint Status
Website accessible in US	Insufficient alone	True, but insufficient
Sales to US residents	Significant factor	None (software is free)
Targeted advertising	Strong evidence	None
U.S. based infrastructure	Relevant factor	Minimal
Knowledge of US users	Can establish "express aiming"	Mere knowledge insufficient

Table 42

In the Linux Mint case, these requirements are not met. The developer has no contacts with the US, no sales, no targeting, and no purposeful availment. Therefore, US courts never obtain jurisdiction in the first place.

The jurisdictional limits of state laws are further illustrated by the parallel to California's Proposition 65. As one commentator observed, "California cannot impose their laws outside of their own jurisdiction. There's a reason that products sold in my country don't carry Prop 65 labels, and there's a reason that most products sold in America don't, either. If it were that simple the California AG would be suing people left, right, and centre for failing to comply with Prop 65 labeling legislation outside of state" (Dawe, 2026 comment section). The same principle applies to age assurance laws: they cannot reach developers who have no contacts with the state, regardless of whether their software is accessible to California residents.

14.3 The European Developer Reality

European developers of open source software like Linux Mint (developed in Ireland by Clem) are not subject to US law because they lack any connection to the United States. Under established US constitutional law, mere accessibility of a website in a jurisdiction does not establish personal jurisdiction over the operator. US courts would have no basis to exercise authority over an Irish developer with no contacts whatsoever with the United States.

14.4 The Practical Result

Element	Reality
Developer Compliance	None required for foreign projects
Developer Risk	Zero, no enforcement possible
User Access	US residents download and use Linux Mint freely
US Government Response	None, no legal leverage exists

Table 43

As Nestor (2026) notes, this is becoming a global standard, with the Digital Services Act (DSA) already in full effect across the EU as of February 2024. However, EU law operates under different principles, and European governments remain hostile to US regulatory overreach.

14.5 European Governmental Hostility to US Enforcement

European governments would be actively hostile to any US enforcement attempt against their citizens. This hostility rests on several foundations:

- **Sovereignty:** European nations do not recognize the authority of the United States to regulate their lawfully resident citizens
- **Clashing values:** US age collection mandates and platform regulation conflict with **GDPR (General Data Protection Regulation)** privacy norms
- **Diplomatic protocol:** International enforcement requests must flow through formal diplomatic channels
- **Public policy exception:** European courts would refuse enforcement of US judgments as contrary to fundamental EU privacy norms

14.6 The Hardware Attestation Jurisdictional Question

Hardware attestation raises novel jurisdictional questions that represent a fundamental shift from the current enforcement model. Under the current **developer-focused phase**, enforcement requires personal jurisdiction over foreign developers—a standard that European projects like Linux Mint easily evade due to lack of US contacts. However, under a future **hardware-focused phase**, enforcement shifts from developers to hardware manufacturers and device sales. If a device's TPM is programmed to accept only US-certified operating systems, that restriction is baked into the hardware itself, regardless of where the device is ultimately used. A European user who purchases a US-manufactured device could find themselves unable to run European open source software. This extraterritorial reach may trigger international disputes and trade complaints, but the hardware itself—once manufactured—enforces US regulatory choices globally. This

transition from personal jurisdiction over developers to physical jurisdiction over devices represents the endgame described in Part XIX.

14.7 International Trade Law Implications

Hardware attestation raises significant international trade law questions beyond the jurisdictional analysis in Section 14.6. Under the **WTO (World Trade Organization)** 's Technical Barriers to Trade (TBT) Agreement, regulations that mandate specific technical specifications for products must not create unnecessary obstacles to international trade and must be no more trade-restrictive than necessary to fulfill legitimate objectives.

WTO Obligation	Potential Violation
National Treatment (Art. III)	US-manufactured devices comply; foreign devices may be blocked
Necessity Test (Art. XX)	Is hardware attestation the least trade-restrictive means?
Technical Regulation (TBT Art. 2)	Certification requirements could be challenged as unnecessary barriers
Legitimate Objectives	Are age verification and surveillance legitimate objectives?

Table 44

The EU, in particular, could challenge US hardware attestation requirements as violations of WTO obligations, especially if they effectively block European open source software from running on US-manufactured devices. This would escalate the sovereignty clash beyond diplomatic protest into formal trade dispute resolution.

14.8 Digital Sovereignty as Framework

European resistance to US age assurance laws can be understood through the lens of **digital sovereignty**—the assertion of national or regional control over digital infrastructure, data, and technologies. The EU's Gaia-X project, aimed at reducing dependence on US cloud providers, exemplifies this approach.

Sovereignty Dimension	EU Position	US Law Implication
Infrastructure	European hosting, European control	Hardware attestation would extend US control to European devices
Data	GDPR restricts data transfer	Age assurance data would flow to US servers
Regulatory	EU law governs EU citizens	US states attempting to regulate EU developers
Technological	European standards preferred	US-mandated certification requirements

Table 45

Digital sovereignty explains why European governments are not merely passive recipients of US regulatory choices but active resisters. Hardware attestation that blocks European open source software on US devices would be viewed as an infringement of European digital sovereignty, likely triggering retaliatory measures.

14.9 Europe's Sovereignty Assertion

The European Parliament's November 2025 adoption of a child safety blueprint represents a direct assertion of digital sovereignty in the face of U.S. pressure. Two days after U.S. Secretary of Commerce Howard Lutnick visited Brussels calling for regulatory rollback, the Parliament moved decisively in the opposite direction (Renew Europe, 2025).

The language from Renew Europe **MEP (Member of European Parliament)** Stéphanie Yon-Courtin is unequivocal: "Europe is sovereign, it is not a regulatory colony. Our digital laws are not for sale. We will not back down on children's protections because a foreign billionaire or Big Tech tells us to" (Renew Europe, 2025). Her colleague Veronika Cifrová Ostrihoňová MEP added: "Under no circumstances can children's wellbeing be used as a bargaining chip in negotiations with platforms or foreign governments. Europe will not lower its standards" (Renew Europe, 2025).

The Parliament's report calls for "age-verification mechanisms that are accurate, privacy-preserving and harmonized at EU level"—a framework that could either align with or conflict with US approaches. This assertion of sovereignty strengthens the digital sovereignty framework developed in Section 14.8 and suggests that Europe will resist US regulatory overreach while pursuing its own parallel path toward age verification infrastructure.

14.10 EU Hardware Attestation Research

The EU is not merely considering age verification policy; it is actively funding development of the hardware infrastructure that would enable it. The **SPIRS (Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process)** project, funded under the Horizon 2020 program, is designing a platform that integrates "a hardware dedicated Root of Trust (**RoT**)" and a processor core with the capability of offering a full suite of security services" (SPIRS Project, n.d.).

The project explicitly aims to support "privacy-respectful attestation mechanisms" and includes "**TEE (Trusted Execution Environment)**, secure boot, and runtime integrity" (SPIRS Project, n.d.). While framed as security research, the technologies being developed—hardware root of trust, attestation mechanisms, secure boot—are identical to those that would enable the hardware attestation endgame described in Part XIX. The EU is building the infrastructure for hardware-enforced compliance even as it asserts sovereignty against US regulatory pressure.

Part XV: The Global Template

15.1 International Convergence Toward Age Verification

The United States is not alone in building age verification infrastructure. The global trend validates the concern about permanent, portable identity systems.

Jurisdiction	Development	Significance
European Union	EU Digital Identity Regulation requires each member state to implement an interoperable digital wallet allowing individuals to prove age without revealing additional information (Electronic Frontier Foundation, 2025)	Portable, reusable identity infrastructure
Australia	Privacy Act reforms include age verification obligations and significantly higher penalties; social media ban for under-16 (eSafety Commissioner, 2026)	Comprehensive age verification mandate
China	On December 29, 2025, China's Cyberspace Administration (CAC) issued an announcement requiring all entities processing minors' data to conduct annual compliance audits and submit a report by January 31, 2026, with penalties for violations potentially reaching 5% of annual turnover under China's Personal Information Protection Law (Hogan Lovells, 2026).	Ongoing surveillance infrastructure

Table 46

15.2 The Portable Identity Vision

FTC Commissioner Meador's endorsement of "one-time, centralized age verification" that can be "portable and used across different platforms" (Federal Trade Commission, 2026b) aligns perfectly with international developments. The vision is a single age verification that follows the user everywhere.

This is exactly the infrastructure this report has identified as the endgame.

15.3 EU Policy Convergence Confirmed

The **FOSDEM (Free and Open Source Software Developers' European Meeting)** 2026 conference featured a session explicitly titled "Age verification: a threat to the open-source ecosystem," confirming that the concerns raised in this report are not limited to the United States (FOSDEM, 2026). The EU's draft **CSA (Child Sexual Abuse)** Regulation ("chat control") contains provisions that would make age verification effectively mandatory for online communications providers and app stores. Proposals for a minimum social media age range from implementation at the platform level to app stores to **operating systems**—the identical approach taken by California and Colorado.

As the FOSDEM session summary warns: "Mandatory age verification at the OS level could pose insurmountable problems for open source operating systems." Projects relying on distributed software distribution systems "would be forced to either thoroughly test every application they offer in advance or, even worse, completely centralize for the sake of age verification." Most critically, "age verification could threaten users' ability to install apps outside of proprietary app stores" (FOSDEM, 2026). The EU is following the same trajectory as the United States, validating the global convergence thesis advanced in Section 15.1.

15.4 Self-Sovereign Identity as an Alternative

Academic research points toward a potential alternative to the government-controlled identity systems that age assurance laws envision. A 2024 paper in the Journal of Information Processing describes self-sovereign identity (**SSI**) systems utilizing attested execution secure processors (**AESPs**) that could provide Sybil-resistant identity verification while preserving user control (Suzuki, 2024).

The proposed system leverages hardware-assisted security that "has become a norm" in mobile devices to enable privacy-respecting attestation without relying on centralized authorities or complex **MPC (Multi-Party Computation)** (Suzuki, 2024). This research demonstrates that the technical infrastructure for age verification need not result in government-controlled identity systems. Privacy-preserving, user-controlled alternatives exist—but they are not being pursued by the legislators drafting age assurance laws.

15.5 The French Alternative: A Different Regulatory Approach

France has implemented similar but distinct legislation since 2024, providing a useful comparison to the US approach. French law requires all new connected consumer devices (computers, phones, smartwatches, etc.) to include parental control software or settings at no extra cost, with users prompted to set it up on first launch ([Service-Public.fr](#), 2024).

Key differences from the US model include:

Feature	US Approach	French Approach
Scope	Operating systems	All connected consumer devices
Data Collection	Mandatory age collection	No age collection required
Verification	Age attestation	Parental control setup
Technical Mandate	Specific API requirements	Functional requirement only
Enforcement	Civil penalties	Device certification (ANFR oversight)

Table 47

Notably, French law includes an explicit exception for devices sold *without* an operating system, recognizing that not all computing devices fit the account-based model ([Service-Public.fr](#), 2024). This alternative approach demonstrates that age-appropriate protections can be implemented without mandatory data collection, OS-level age signals, or the surveillance infrastructure the US model requires. It provides a potential template for privacy-preserving compliance that the US has not pursued.

Part XVI: The Federal Pipeline

16.1 State as Laboratory, Federal as Implementation

The concern that state laws are experiments for federal adoption is validated by the introduction of the federal App Store Accountability Act, which would preempt state laws (Loeb & Loeb LLP, 2025). Davis Wright Tremaine LLP (2026) describes a "wave of federal 'online safety' legislation" hitting Congress, with 19 bills under consideration.

16.2 The Age Verification Study as Trojan Horse

KOSA's Sec. 107 requires the Secretary of Commerce, in coordination with the **FCC (Federal Communications Commission)** and FTC, to conduct a study evaluating the most technologically feasible methods and options for developing systems to **verify age at the device or operating system level** (Kids Online Safety Act, S. 1748, 119th Cong. § 107, 2025; Davis Wright Tremaine LLP, 2026; La Discussionne, 2026).

The study must consider:

- Benefits of device/OS level age verification (Kids Online Safety Act, S. 1748, 119th Cong. § 107(b)(1), 2025)
- What information may need to be collected (Kids Online Safety Act, S. 1748, 119th Cong. § 107(b)(2), 2025)
- Accuracy and accessibility impacts (Kids Online Safety Act, S. 1748, 119th Cong. § 107(b)(3), 2025)
- How to verify age while mitigating privacy and data security risks (Kids Online Safety Act, S. 1748, 119th Cong. § 107(b)(4), 2025)
- Technical feasibility, including the need for potential hardware and software changes (Kids Online Safety Act, S. 1748, 119th Cong. § 107(b)(5))
- Impact on competition and barriers to entry for small companies (Kids Online Safety Act, S. 1748, 119th Cong. § 107(b)(6), 2025)

The danger: A study finding that OS level age verification is "technologically feasible" and "can be done with privacy protections" would provide the justification for a future federal mandate. The state laws serve as real world experiments; the study serves as the official recommendation. The explicit mention of "hardware and software changes" in the study's scope confirms that hardware attestation is under active consideration.

16.3 The Hardware Attestation Endgame (Expanded)

A federal law based on the KOSA Sec. 107 study could:

- **Require TPM-based validation** of operating system certificates at boot time
- **Establish a National Software Certification Authority** to issue certificates to compliant operating systems
- **Mandate that all new devices** include hardware capable of cryptographic attestation
- **Require ISPs to block** non-attested devices from network access
- **Include statutory prohibitions** on circumventing, disabling, or tampering with attestation mechanisms, and on manufacturing or distributing tools designed for such purposes
- **End general purpose computing** as currently understood

- **Make open source operating systems impossible to use** on new devices, regardless of user sophistication

Unlike software-level compliance, which can be ignored by foreign developers and circumvented by technical users, hardware attestation creates a physical barrier that cannot be bypassed without replacing the device itself. This is the end of practical impunity.

16.4 The Statutory Prohibition Model

Any future federal legislation establishing hardware attestation would almost certainly include provisions explicitly criminalizing:

- **Circumvention:** Bypassing, disabling, or tampering with the attestation mechanism
- **Tools:** Manufacturing, distributing, or providing tools designed to circumvent attestation
- **Modification:** Altering hardware or firmware to defeat attestation checks
- **False Certification:** Obtaining or providing fraudulent cryptographic certificates

These provisions would function similarly to the **DMCA (Digital Millennium Copyright Act)**'s anti-circumvention rules but would be specific to the attestation regime and enforceable through the same regulatory framework (FTC, DOJ, or a dedicated agency). Unlike the DMCA, which requires a nexus to copyright infringement, these provisions would directly target interference with government-mandated compliance infrastructure.

Precedent: The DMCA's anti-circumvention provisions (17 U.S.C. § 1201) provide a legislative template for how Congress might structure such prohibitions, including:

- Bans on circumvention of technological measures
- Bans on trafficking in circumvention tools
- Civil and criminal penalties
- Exceptions through administrative rulemaking

However, the actual authority would derive from the attestation statute itself, not from existing copyright law.

16.5 The Preemption Question

Lima-Strong (2025) reports that Democratic lawmakers panned the GOP-led committee's approach to state regulation across many of the bills under consideration, arguing it would override far too many state-level child safety laws. Kate Ruane of the Center for Democracy and Technology testified that she feared the broad preemption language sought by Republicans could lead to "children having less protections at the state level than they do today" (Lima-Strong, 2025).

16.6 Technology-Forcing Regulation

The age assurance laws can be understood as **technology-forcing regulation**—a strategy that mandates performance standards requiring technological innovation rather than simply codifying existing practices. Common in environmental and safety law, technology-forcing regulation aims to accelerate development of beneficial technologies.

In this context, the laws force development of:

- OS-level age attestation interfaces
- Real-time age signal APIs
- Hardware-based verification systems
- Portable digital identity infrastructure

The KOSA Sec. 107 study explicitly contemplates "hardware and software changes," confirming that technology-forcing is intended. However, unlike environmental regulation where innovation benefits public health, here the forced innovation primarily enables surveillance and market consolidation. The technology-forcing frame also explains why compliance costs are so high: the mandated technologies did not previously exist and require significant development investment.

Part XVII: The Double Hidden Action

17.1 Beyond Accidental Damage

The observation that this combined state federal framework represents more than accidental damage to open source merits serious consideration:

Layer	Apparent Purpose	Hidden Effect
Surface	Child protection	Public support
First Hidden	OS level age mandate (California/Colorado)	Compliance infrastructure at device level
Second Hidden	Platform regulation (KOSA)	Compliance infrastructure at service level
Third Hidden	App store verification (Texas/Utah/Louisiana)	Identity verification infrastructure
Fourth Hidden	COPPA expansion and enforcement	Detailed, impossible compliance requirements
Fifth Hidden	Open source marginalization	Privatization pressure
Sixth Hidden	National security framing	Control justification
Seventh Hidden	Surveillance enablement	Elimination of privacy preserving alternatives
Eighth Hidden	Federal study (KOSA Sec. 107)	Pathway to hardware attestation
Ninth Hidden	International convergence (EU Digital Identity)	Global portable identity system
Tenth Hidden	Market transfer mechanism	Corporate monopoly and rising consumer costs

Table 48

17.2 The Cumulative Effect

Whether intentional or merely convergent, the combined framework's effects cascade:

1. **California/Colorado OS mandates** require device level compliance infrastructure
2. **Texas/Utah/Louisiana app store laws** require identity verification infrastructure
3. **KOSA platform mandates** require service level compliance infrastructure
4. **COPPA** requires detailed security programs, data retention policies, and parental consent mechanisms
5. **Compliance costs** exclude small players at all levels (see Section 5.4)
6. **Liability risks** deter volunteers

7. **Platform enforcement** (app store removal) enforces compliance where government cannot
8. **National security concerns** justify further restrictions
9. **Market pressure** favors corporate solutions
10. **Regulatory capture** benefits large corporations
11. **Open source** becomes legally non-viable at OS, app store, and platform levels
12. **Open source projects geoblock or shut down**, transferring market share to corporate alternatives
13. **Corporate market share increases**, enabling monopoly pricing
14. **Consumer costs rise** (monetary and privacy)
15. **Hardware attestation study** (KOSA Sec. 107) lays groundwork for physical enforcement
16. **Future federal hardware mandate** would make open source impossible to run on new devices
17. **All software** eventually requires corporate backing
18. **Control** centralizes in entities government can regulate and compel
19. **Identity verification** becomes universal
20. **Surveillance** becomes continuous and unavoidable
21. **Anonymous computing** ends

17.3 The End of General Purpose Computing

The logical endpoint of this trajectory is the elimination of general purpose computing as we know it, replaced by **special purpose appliances** that can only run government approved software on government verified identities, with all activity continuously reported to corporate servers and available to government agencies on demand.

Part XVIII: Recommendations and Considerations

18.1 For Open Source Communities

- **Consider EU Legal Structure:** Projects should consider establishing themselves as EU based legal entities (Irish foundations, German nonprofits, etc.) to gain the protection of European sovereignty and GDPR. Linux Mint's structure in Ireland provides a model. This positions the project beyond US jurisdiction, as analyzed in Part XIV.
- **Host Infrastructure in EU:** Keep code repositories, build systems, and distribution servers on European soil, beyond the reach of US court orders.
- **Consider Technical Responses:** Geoblocking US IP addresses, as MidnightBSD has done with California (Nestor, 2026), may be the only practical option for projects unwilling to risk US liability. However, recognize that each geoblocking announcement transfers market share to corporate alternatives.
- **Monitor All Levels:** Track state bills, federal legislation, COPPA rulemaking, and international developments simultaneously; they are coordinated.
- **Build Relationships:** Establish contacts with civil liberties organizations and privacy advocates.
- **Prepare Messaging:** Frame opposition as privacy protection, resistance to warrantless surveillance, and opposition to government-facilitated monopolies, not anti-child safety.
- **Document Contributions:** Maintain clear records of contributor diversity to counter "foreign control" narratives.
- **Highlight Security Benefits:** Emphasize that open source transparency enables security auditing and prevents hidden surveillance.
- **Engage in Rulemaking:** Where possible, participate in agency rulemaking processes to shape implementation.
- **Challenge Regulatory Moats:** Raise antitrust concerns about government-created barriers to entry that favor corporate entities.
- **Oppose Hardware Attestation:** Explicitly advocate against provisions that would enable hardware-level validation of operating systems, highlighting the impact on innovation, competition, and user autonomy.

- **Coordinate Legal Defense:** Build relationships with organizations like EFF, ACLU, and Software Freedom Law Center to support potential developer defense.

18.2 For Policymakers

- **Exempt Open Source:** Create clear exemptions for open source and community distributions at both state and federal levels, including from COPPA's detailed requirements.
- **Narrow Definitions:** Fix the "primary user" problem in state bills; narrow federal bills' broad platform definitions.
- **Add Privacy Protections:** Explicitly prohibit data retention, warrantless access, and surveillance collaborations.
- **Remove the Age Verification Study:** KOSA Sec. 107 is a pathway to hardware attestation; it should be eliminated.
- **Reject Hardware Attestation Mandates:** Oppose any requirement for hardware-level validation of operating systems, which would eliminate open source and entrench corporate monopolies.
- **Reject Sweeping Preemption:** Avoid language that would eliminate stronger state protections.
- **Consider Constitutional Vulnerabilities:** Learn from state laws that have been enjoined on First Amendment grounds.
- **Sunset Provisions:** Require reauthorization to prevent mission creep.
- **Address the Parenting Question:** Acknowledge that technology cannot replace active parenting.
- **Reject the Portable Identity Vision:** Resist calls for centralized, reusable age verification that follows users across platforms.
- **Examine Antitrust Implications:** Investigate whether government-created regulatory moats that exclude non-corporate actors violate principles of fair competition.
- **Adopt Just Transition Principles:** Recognize open source as a public good and design regulations to preserve it, analogous to "just transition" provisions in environmental law.

18.3 For Users

- **Choose European Software:** Prioritize open source software developed and hosted in Europe, such as Linux Mint, which operates beyond US jurisdiction. By using software from EU based projects, you benefit indirectly from European legal protections even though you cannot invoke them directly.
- **Understand the Laws:** Know your rights and the actual requirements of both state and federal proposals.
- **Contact Legislators:** Express concerns about privacy, surveillance, open source impact, and rising consumer costs at all levels.
- **Consider Technical Literacy:** Learn to use VPNs and alternative DNS if blocking occurs.
- **Stockpile Hardware:** Purchase pre-2028 devices while they remain available, recognizing that hardware attestation on future devices will eliminate the ability to run non-compliant operating systems.
- **Support Advocacy:** Donate to EFF, ACLU, and open source organizations fighting surveillance and monopolization.
- **Resist Fear Mongering:** Question national security claims about open source.
- **Recognize the Stakes:** The elimination of open source is the elimination of the last privacy preserving option and the last constraint on corporate pricing.
- **Consider Civil Disobedience:** As hardware attestation approaches, organized resistance may become necessary.

18.4 For Parents

- **Parent, Don't Delegate:** Neither state laws nor federal legislation can replace active parenting. The duty cannot be shifted to operating systems or platforms.
- **Stay Involved:** Monitor your children's online activity directly. Know what platforms they use, who they communicate with, and how much time they spend.
- **Teach Digital Literacy:** Help children understand online risks and privacy rights. Equip them to make their own decisions rather than relying on algorithmic enforcement.

- **Resist False Security:** OS level age signals and platform parental tools do not protect children from all harms. They create a false sense of security while building surveillance infrastructure.
 - **Question Government Motives:** Ask why the state and federal government want your family's data, why they are eliminating free alternatives, and what else the infrastructure might be used for.
 - **Use Open Source:** Support and use open source software where possible. It remains the only computing environment that doesn't automatically report back to corporate and government databases.
-

Part XIX: The Hardware Attestation Endgame and the End of Impunity

19.1 The Current Reality: User Impunity

As currently structured, both state laws and federal proposals contain **no user liability**. US residents face no penalty for downloading, installing, or using non-compliant open source operating systems and software—**for now**. Technical users can easily bypass any potential ISP-level blocking through VPNs, alternative DNS, or direct downloads from foreign mirrors. European-developed open source software like Linux Mint remains freely available and usable regardless of US law—**for now**.

This creates a situation where, for the foreseeable future, determined users can still access open source operating systems and software. The only entities that will comply are large corporations with US-based assets that can be targeted by regulators. This is the **practical impunity** that open source projects and their users currently enjoy—but it is temporary, as Section 19.2 explains.

19.2 The Hardware Attestation Endgame

This impunity is temporary. It exists only because the current regulatory framework relies on software-level compliance and ISP-level blocking, both of which are easily circumvented. The endgame, already visible in federal studies and international developments, is **hardware-level attestation** that would fundamentally alter this dynamic, shifting from the current developer-focused enforcement model to a hardware-focused model that cannot be bypassed.

What Hardware Attestation Means:

Hardware attestation refers to a system where a computer's hardware (typically a Trusted Execution Module or similar secure coprocessor) verifies that the software being loaded—starting with the operating system itself—is authorized, certified, and compliant with applicable laws before allowing the system to boot or connect to networks.

Current System	Hardware Attestation System
Software checks compliance	Hardware checks compliance
Can be bypassed by modifying software	Cannot be bypassed without replacing hardware
User controls what runs	Hardware vendor/government controls what runs
Open source can run unmodified	Open source must be cryptographically signed
Circumvention is technical but possible	Circumvention is impossible or criminal

Table 49

19.3 How Hardware Attestation Would Function

Under a hardware attestation regime:

1. **Manufacturing Stage:** All new computing devices are manufactured with a Trusted Execution Module (**TPM**) or equivalent secure hardware that stores cryptographic keys and performs secure boot validation.
2. **Certification Stage:** Operating system vendors must obtain cryptographic certificates from a government-authorized body (such as a National Software Certification Authority). This certification confirms that the OS complies with all applicable age verification, data collection, and content restriction laws.
3. **Boot Validation Stage:** When the device boots, the TPM checks the cryptographic signature of the bootloader and operating system against a list of approved certificates. If the signature is missing, invalid, or revoked, the device **refuses to boot** or enters a restricted recovery mode.
4. **Software Validation Stage:** Beyond the OS, the TPM may also validate drivers, kernel modules, and even applications against approved certificates before allowing them to execute.
5. **Network Access Stage:** Internet service providers may be required to verify that connecting devices have valid hardware attestation before granting network access, creating a second layer of enforcement.

19.4 The Legal Framework for Hardware Attestation

While no current law mandates hardware attestation, the pathway is being constructed:

Law/Provision	Role in Hardware Attestation Pathway
KOSA Sec. 107	Requires study of "device or operating system level age verification systems," including "technical feasibility, including the need for potential hardware and software changes" (Kids Online Safety Act, S. 1748, 119th Cong. § 107, 2025)
FTC Policy Statement	Endorses "one-time, centralized age verification" that can be "portable and used across different platforms" (Federal Trade Commission, 2026b)
EU Digital Identity Regulation	Requires member states to implement interoperable digital wallets; provides infrastructure for portable identity
State OS Mandates	Create the expectation that operating systems should verify age at the device level
COPPA's "Actual Knowledge"	Creates liability that incentivizes automated, hardware-level solutions
SPIRS Project (EU)	Developing hardware root of trust and attestation mechanisms (SPIRS Project, n.d.)

Table 50

19.5 Why Hardware Attestation Eliminates Open Source

Hardware attestation is structurally incompatible with community open source development:

Open Source Characteristic	Hardware Attestation Requirement	Conflict
Anyone can modify and rebuild code	Only cryptographically signed code runs	Modification becomes impossible
Distributed development, no central authority	Centralized certification authority required	No entity to obtain certificates
Users control their own devices	Hardware vendor/government controls boot process	User autonomy eliminated
Privacy-respecting modifications possible	Attestation ensures compliance with data collection	Surveillance enforced at hardware level
Zero monetary cost	Certification fees, insurance, legal entity required	Economic barrier to entry

Table 51

19.6 The Tipping Point: When Impunity Ends

The practical impunity that open source users currently enjoy will end when three conditions are met:

1. **Widespread Hardware Adoption:** New devices with TPM 2.0 or equivalent become the standard, making attestation technically possible for most users.
2. **Federal Attestation Mandate:** A federal law requires hardware-level validation, using the KOSA Sec. 107 study as justification.
3. **Network Access Enforcement:** ISPs are required to block non-attested devices, closing the VPN/workaround loophole.

Timeline Estimate:

Phase	Timeline	Status
Hardware capability	Already present (TPM 2.0 in most new devices)	Existing
State OS mandates	2027-2028	California, Colorado
Federal study	2026-2027	KOSA Sec. 107
Federal recommendation	2027-2028	Based on study findings
Federal mandate	2029-2030	Projected
Network enforcement	2030+	Projected

Table 52

19.7 The Consumer Trap

Hardware attestation creates a consumer trap that is nearly impossible to escape:

Attempt to Escape	Obstacle
Use older hardware	Hardware eventually fails; no new drivers; security vulnerabilities
Build custom hardware	Impossible for average user; expensive; may still require network attestation
Use foreign hardware	May be blocked at network level; import restrictions
Use VPN to bypass network blocks	Attestation occurs at boot, before network connects
Modify TPM	Would require specialized equipment and expertise; technically extremely difficult

Table 53

Questions about edge cases highlight the absurdity of applying these laws to modern computing environments. As one commenter noted regarding containerized applications, "what about Docker containers? Do I need to enter my age for every single Docker container that gets created? In companies they get created and destroyed by the thousand each day. This is beyond ridiculous" (Dawe, 2026 comment section). Containers, virtual machines, and ephemeral computing environments do not fit the "user account" model that age assurance laws assume. Yet under the broad definitions of "operating system provider" and "device," they could be swept into the compliance regime, creating impossible technical and operational burdens for cloud infrastructure providers and DevOps environments.

19.8 The Statutory Prohibition Layer

Any future federal legislation establishing hardware attestation would almost certainly include provisions explicitly criminalizing:

- **Circumvention:** Bypassing, disabling, or tampering with the attestation mechanism
- **Tools:** Manufacturing, distributing, or providing tools designed to circumvent attestation
- **Modification:** Altering hardware or firmware to defeat attestation checks
- **False Certification:** Obtaining or providing fraudulent cryptographic certificates

These provisions would function similarly to the DMCA's anti-circumvention rules but would be specific to the attestation regime and enforceable through the same regulatory framework (FTC, DOJ, or a dedicated agency). Unlike the DMCA, which requires a nexus to copyright infringement, these provisions would directly target interference with government-mandated compliance infrastructure.

Precedent: The DMCA's anti-circumvention provisions (17 U.S.C. § 1201) provide a legislative template for how Congress might structure such prohibitions, including:

- Bans on circumvention of technological measures
- Bans on trafficking in circumvention tools
- Civil and criminal penalties
- Exceptions through administrative rulemaking

However, the actual authority would derive from the attestation statute itself, not from existing copyright law.

19.9 The Impossibility of Dual Boot

Hardware attestation does not necessarily prevent dual booting—but it requires that **every** bootable operating system be certified. A user could theoretically dual boot Windows and a certified version of Ubuntu, but they could not boot an uncertified community distribution. The open source operating system must become a certified, compliant product to run at all.

19.10 Summary: The End of Impunity

Current Situation	Hardware Attestation Future
Open source runs on any hardware	Open source runs only if certified
Users can bypass blocks with VPNs	Network blocks all uncertified devices
Technical users can always find a way	No way exists for any user
Impunity is real	Impunity ends
Open source survives through foreign hosting	Open source cannot run on new US devices

Table 54

The practical impunity that currently protects open source users is temporary. It exists only because the regulatory infrastructure is incomplete. Each new law, each new study, each new technological development closes another loophole. The hardware attestation endgame, when fully implemented, will make open source operating systems impossible to run on any new device sold in the United States, regardless of the user's technical sophistication.

19.11 Intergenerational Equity

The hardware attestation endgame raises questions of **intergenerational equity**—the fairness of decisions that constrain future generations' choices. If fully implemented, hardware attestation will mean that users born after 2030 will never experience general-purpose computing. They will inherit a world where devices only run approved software, where every action is surveilled, and where modification is impossible.

Generation	Computing Experience
Pre-2028	General-purpose computing; open source options available
Transition (2028-2032)	Older hardware runs open source; new hardware locked
Post-2032	Hardware attestation universal; open source unavailable

Table 55

This creates an irreversible path dependency: once the open source ecosystem withers due to lack of users and contributors, it cannot be revived even if future generations desire it. The decision to eliminate open source is being made by one generation but will constrain all future generations.

19.12 Environmental Impact

Hardware attestation would have significant environmental consequences. If new devices are required to have TPM 2.0 or equivalent attestation capability, and if network access is conditioned on attestation, users of pre-attestation hardware face three choices:

1. Continue using older devices offline
2. Replace devices prematurely
3. Accept surveillance by migrating to certified OSES

Outcome	Environmental Impact
Premature replacement	Millions of functional devices become e-waste
Offline use	Reduced utility; digital divide implications
Continued online use	Requires accepting surveillance

Table 56

The **UN (United Nations)** estimates global e-waste at 50 million metric tons annually. Hardware attestation mandates would add significantly to this burden, forcing replacement of devices that would otherwise remain functional. This conflicts with sustainability goals and circular economy principles, and disproportionately affects low-income users who rely on older hardware.

Part XX: Conclusion

20.1 The Entrenched Reality

The analysis in this report is no longer a warning about future possibilities. As of March 2026:

- **Texas, Utah, and Louisiana** have laws taking effect in 2026 (Loeb & Loeb LLP, 2025)
- **California's AB 1043** takes effect January 1, 2027 (James, 2026)
- **COPPA's strengthened amendments** are effective April 22, 2026 (Federal Trade Commission, 2026a)
- **At least 19 federal bills** are under active consideration (Davis Wright Tremaine LLP, 2026)
- **Linux distributions** are actively discussing compliance or geoblocking (Nestor, 2026; James, 2026; Dawe, 2026)
- **Google and Apple** have launched age verification APIs (Loeb & Loeb LLP, 2025)

- **The FTC** has issued a policy statement encouraging age verification technologies (Federal Trade Commission, 2026b)
- **The Supreme Court** has upheld state age verification laws (Davis Wright Tremaine LLP, 2026)
- **MidnightBSD** has already chosen to exclude California users, demonstrating the market transfer mechanism in action (Nestor, 2026; Ridley, 2026)
- **The DB48x calculator project** has also chosen geoblocking, demonstrating the law's absurd reach (Ridley, 2026)
- **KOSA Sec. 107** mandates a study of device-level age verification, including hardware changes, laying the groundwork for federal hardware attestation
- **The EU** is actively considering OS-level age verification and funding hardware root of trust research (FOSDEM, 2026; SPIRS Project, n.d.)
- **Open source economic value** is estimated at \$8.8 trillion, underscoring the stakes of market transfer (Open Source Initiative, 2026)

20.2 The Bill's Multiple Layers

The combined framework operates on multiple levels:

Surface Level: Child protection through age based restrictions and platform safeguards

- Appears reasonable
- Appeals to bipartisan concern for minors
- Difficult to oppose publicly

Structural Level: Regulatory framework with profound implications

- Creates infrastructure for digital ID at OS level (California/Colorado)
- Creates identity verification infrastructure at app store level (Texas/Utah/Louisiana)
- Creates family surveillance infrastructure at platform level (KOSA)
- Creates detailed compliance infrastructure at federal level (COPPA)
- Imposes costs fatal to open source at all levels
- Establishes comprehensive surveillance architecture
- Tests state and federal power over global internet

Market Level: Systematic transfer of market share from open source to corporate entities

- Open source projects forced to geoblock or shut down
- Users migrate to corporate alternatives
- Corporate monopoly power increases
- Consumer prices rise
- Privacy becomes a premium product
- **\$8.8 trillion in economic value at stake** (Open Source Initiative, 2026)

Philosophical Level: Government replacing parental authority

- Assumes parents cannot be trusted
- Shifts responsibility to corporations and regulators
- Undermines family autonomy

National Security Level: Template for control

- Echoes TikTok divestiture logic
- Provides framework for labeling open source as "risky"
- Justifies privatization through security concerns

Surveillance Level: Infrastructure for mass monitoring

- Eliminates privacy preserving alternatives at OS, app store, and platform levels
- Ensures all devices run software that reports back
- Ensures all platforms have parental surveillance tools
- Creates data pipelines accessible to law enforcement
- Normalizes continuous monitoring as "compliance"

Hardware Level: The end of impunity

- Federal study of hardware attestation underway
- EU funding hardware root of trust research (SPIRS Project, n.d.)
- Future mandate would cryptographically lock devices to certified operating systems
- Open source becomes impossible to run on new US devices

- User autonomy eliminated at hardware level

International Level: Global convergence toward portable identity

- EU Digital Identity wallets
- Australian age verification mandates
- Chinese compliance audits
- EU policy converging on OS-level age verification (FOSDEM, 2026)
- French alternative model with no mandatory data collection ([Service-Public.fr](#), 2024)

20.3 The Unified Theory Validated

The evidence supports a coherent theory: state and federal governments are cooperating with corporations to push open source operating systems and software out of the market. This cooperation serves mutual interests:

- **Governments** gain universal surveillance infrastructure and control over computing environments
- **Corporations** gain market monopoly, pricing power, and elimination of free competitors

The cooperation need not be explicit conspiracy. Convergent interests, industry lobbying, regulatory capture, and structural incentives achieve the same result. When MidnightBSD excludes California users, it is not just protecting itself from liability. It is ceding its user base to corporate alternatives. Those users will migrate to Windows, macOS, or corporate-backed Linux distributions. The market transfer is real. The rising costs are inevitable. The surveillance is universal. The economic stakes are measured in trillions of dollars.

20.4 The Antitrust Paradox

This arrangement would be illegal if done by corporations alone. Yet because government action creates the regulatory barriers, it is exempt from antitrust scrutiny. The same agencies that enforce antitrust laws are participating in creating these regulatory moats. The same legislators who decry Big Tech monopoly power are voting for laws that entrench it. The same arguments used against monopolists will be validated by the very laws passed in the name of "protection."

20.5 The Hardware Attestation Endgame

The practical impunity that currently protects open source users is temporary. The KOSA Sec. 107 study explicitly considers hardware changes, and the FTC has endorsed portable, reusable age verification. The EU is simultaneously funding hardware root of trust research. The logical endpoint is hardware-level attestation that would:

- Require cryptographic certification for all operating systems
- Block non-compliant operating systems from booting on new devices
- Criminalize circumvention
- Make open source operating systems impossible to run on any new US device
- End general purpose computing as currently understood

20.6 The Parenting Question

At its core, this combined framework represents a fundamental shift in the relationship between family and state. **As this report contends, this is effectively parents not parenting their kids so the government comes in for the safety of children to do what parents should be doing.**

The question society must answer: **Do we want government raising our children through algorithmic enforcement at the OS, app store, and platform levels, enforced at the hardware level, while simultaneously transferring market power to corporations and eliminating privacy-respecting alternatives?**

20.7 The National Security Trap

The TikTok precedent reveals how quickly "protection" arguments can escalate:

Stage	Rhetoric	Reality
1	"Protect children online"	Age attestation mandate (California/Colorado)
2	"Protect children from apps"	App store verification (Texas/Utah/Louisiana)
3	"Protect children's privacy"	COPPA expansion (Federal)
4	"Protect children from platforms"	Duty of care and safeguards (KOSA)
5	"Protect national security"	Foreign adversary control claims
6	"Protect critical infrastructure"	Open source software restrictions
7	"Protect American way of life"	Universal digital ID requirements
8	"Protect against threats"	Continuous surveillance of all devices
9	"Protect against non-compliant software"	Hardware attestation mandate

Table 57

Each stage is presented as a reasonable response to the previous stage's inadequacies. Each stage transfers more market share to corporate entities. Each stage builds more surveillance infrastructure. Each stage closes another loophole.

20.8 The Surveillance Endgame

The elimination of open source operating systems and software is not merely about compliance. It is about ensuring that every device in America runs software that can be surveilled. The cooperation between government and corporations is well established. Data flows freely from corporate servers to law enforcement databases, often without warrants, often without oversight.

Open source represented the one alternative. Software that didn't have a corporate parent to compel. Code that could be audited to ensure no hidden surveillance. Systems that could be modified to block unwanted data collection.

The privatization of open source, whether through acquisition, compliance costs, or outright prohibition, closes that last loophole. Hardware attestation ensures that no future loophole can open. When all software comes from entities that can be regulated, compelled, and partnered with, and when hardware enforces that only such software can run, surveillance becomes not a possibility but a certainty.

The market transfer mechanism ensures that consumers bear multiple harms:

Type of Harm	Manifestation
Price Harm	Corporate OS prices rise without free competition
Privacy Harm	Surveillance becomes unavoidable
Choice Harm	Only corporate-controlled OSes available
Innovation Harm	Corporate inertia replaces community experimentation
Autonomy Harm	Hardware enforces corporate/government control

Table 58

20.10 The Constitutional Crisis

This framework potentially eviscerates Fourth Amendment protections. If the government mandates that all devices collect and report data, and if that data is available to law enforcement on demand, then the warrant requirement has been effectively nullified. The government is not searching your computer; your computer is already telling the government everything.

Hardware attestation adds a new dimension: the government, through hardware manufacturers, controls what software can even run. This is not just surveillance; it is preemptive control over the computing environment itself.

20.11 The Texas Warning

The preliminary injunction against Texas's "commercially reasonable" law demonstrates that these statutes are not immune to constitutional challenge. The court's conclusion that the law likely violates the First Amendment because it restricts lawful speech and broadly covers nearly all apps without targeting only harmful content should give pause to legislators considering similar measures.

KOSA's duty of care provision faces even greater First Amendment vulnerabilities. Similar challenges could be raised on Fourth Amendment grounds. Hardware attestation, by controlling what software can run, may face even steeper constitutional hurdles.

20.12 The International Reality

The combined framework's enforcement against European open source developers is effectively impossible—for now. Hardware attestation changes this calculus. If US-manufactured devices are programmed to accept only US-certified operating systems, the restriction travels with the hardware. A European user who buys a US laptop may find themselves unable to run European open source software. This extraterritorial reach will

likely trigger international disputes and trade challenges under WTO rules, but the hardware itself enforces US regulatory choices globally.

The European Union, with its GDPR and a demonstrated **hostility toward US regulatory overreach** (Renew Europe, 2025), provides a potential refuge for open source development and for users who can obtain non-US hardware. However, as global supply chains integrate, this refuge may narrow. **While the EU asserts its sovereignty against US pressure** (Renew Europe, 2025), it is simultaneously, through other initiatives, **funding the development of** hardware attestation infrastructure (SPIRS Project, n.d.). France offers an alternative model focused on parental controls rather than mandatory age data collection ([Service-Public.fr](https://www.service-public.fr), 2024).

20.13 The Open Source Question

Whether the combined framework's impact on open source is:

- **Accidental:** Unintended consequence of poorly drafted legislation
- **Intentional:** Deliberate strategy to marginalize uncontrollable software
- **Double Hidden:** Multi-layer attack on open source viability using child protection, national security, and surveillance as justification
- **Market Transfer:** Coordinated state federal strategy to transfer market share to corporate entities
- **Hardware Enforced:** Pathway to eliminate open source at the hardware level

may be less relevant than the **effect**. The outcome is the same regardless of intent: open source software becomes legally non-viable in regulated markets, control shifts to corporations with compliance resources, surveillance becomes structurally inevitable, consumer costs rise, and hardware ensures no escape. **However, as Section 5.5 details, these effects vary significantly by project type: US-based community projects face elimination; EU-based projects may survive by serving US users remotely; corporate-backed projects may adapt through compliance investment; and projects targeting older hardware may persist on pre-attestation devices.**

20.14 The Privacy Future

Nestor (2026) captures the central concern: this is "a profound and dangerous step toward a society in which anonymity in public life becomes a relic of the past."

The report concludes that the trajectory of these laws leads to an inescapable outcome: the government does not need to know a user's age or mandate ID verification at the OS

level when the infrastructure built for "compliance" ensures that information will be retained by companies and made available to government. Once open source is eliminated, there will be no way to verify what data is being collected, no way to stop it from being shared, no free alternatives to constrain corporate pricing, and ultimately, no hardware that will run anything other than approved, surveilled systems.

20.15 The Congressional Warning

The TikTok experience offers a crucial lesson:

"Picking a single company to blame may make for good headlines, but it is not a substitute for comprehensive technology policy" (Collins, 2026).

The same applies to picking a single regulatory mechanism or a single level of government to act. Addressing genuine concerns about child safety, privacy, and security requires comprehensive approaches that respect fundamental rights, not targeted controls that create infrastructure for surveillance, transfer market share to corporations, eliminate free alternatives, and encode control into hardware.

20.16 The Practical Impunity: A Temporary Condition

Both state laws and federal proposals contain no user liability, so US residents face no penalty for using non-compliant software—for now. Technical users can easily bypass any potential ISP blocking through VPNs and alternative DNS—for now. European developed open source software remains freely available and usable regardless of US law—for now.

This practical impunity is a temporary condition, not a permanent refuge. The hardware attestation endgame, when fully implemented, will close these loopholes permanently. The only entities that will comply in the interim are large corporations with US based assets that can be targeted. The only users who will retain access to open source are those who stockpile pre-attestation hardware and never connect to networks that enforce attestation.

20.17 The European Escape Hatch

For those seeking to preserve open source and privacy, the clearest path forward is the one already demonstrated by projects like Linux Mint: structure development and distribution outside US jurisdiction, in countries with strong privacy traditions and sovereign legal systems that do not recognize US regulatory authority. US residents can continue using this software with impunity, as analyzed in Part XIV—until hardware attestation makes it impossible to run on new US devices. The European Union, with its GDPR and hostile stance toward US surveillance overreach, provides the most viable refuge for open source development. For users, the refuge is increasingly limited to older hardware and non-US devices.

20.18 Final Assessment

California AB 1043, Colorado SB 26 051, Texas's and Utah's and Louisiana's app store laws, COPPA's strengthened amendments, and the federal Kids Online Safety Act represent a coordinated, multi-level regulatory strategy that is already entrenched and operational. While framed as child protection, together they establish mechanisms that could eliminate open source software, create comprehensive surveillance infrastructure, transfer market share to corporate entities, enable monopoly pricing, and pave the way for hardware level attestation that would make these changes permanent and inescapable.

The combined framework's practical unenforceability against foreign developers, coupled with its inability to reach users, suggests that open source can survive through international structuring—for now. However, for domestic US based projects, the compliance burden is already fatal. For US based users, the options are increasingly limited to corporate controlled, surveillance enabled, paid operating systems. And for future users, hardware attestation threatens to eliminate choice entirely.

The TikTok controversy demonstrated how quickly "protection" can become "control." The same dynamic applied to open source means the end of software developed by communities rather than corporations, the end of privacy respecting alternatives, the end of the competitive constraint that kept corporate prices in check, and—with hardware attestation—the end of user autonomy over their own devices.

For those who value privacy, anonymity, parental authority, the right to modify their own software, and the ability to use technology without being surveilled or overcharged, these laws and others like them represent not a warning but a present reality: **the future of computing is one where every action is age verified, identity attested, nationally vetted, centrally controlled, continuously surveilled, increasingly expensive, and—ultimately—hardware enforced.**

Whether that future is total depends on the vigilance of those who recognize what is at stake. For now, the simplest defense is also the most effective: use software developed beyond the reach of US regulators, assert the fundamental right to control one's own computing experience without government permission, stockpile hardware while it remains possible, and recognize that the elimination of open source is not an accident but an objective of the coordinated state federal strategy—an objective that serves both government surveillance interests and corporate monopoly interests at the expense of every user.

References

- ABA Journal. (2026, February 19). *Lawyer fees skyrocket; some charge up to \$3,400 per hour*. Retrieved March 3, 2026, from <https://www.abajournal.com/news/article/lawyers-fees-skyrocket-some-charging-up-to-3400-an-hour>
- Anderson P.C. (2025, January 24). *Where TikTok goes next: Navigating the uncertainty of a landmark ban*. Mondaq. Retrieved March 3, 2026, from <https://www.mondaq.com/unitedstates/social-media/1573362/where-tiktok-goes-next-navigating-the-uncertainty-of-a-landmark-ban>
- Benson, P. J., Brannon, V. C., & Lampe, J. R. (2024, May 9). *Regulation of TikTok Under the Protecting Americans from Foreign Adversary Controlled Applications Act: Analysis of Selected Legal Issues* (CRS Product No. LSB11127). Congressional Research Service. Retrieved March 3, 2026, from <https://www.congress.gov/crs-product/LSB11127>
- Buzzi, M. (2026, March 4). *Well, that didn't last: With M5, the MacBook Air is back to \$1,099. Why?* PCMag. Retrieved March 4, 2026, from <https://www.pcmag.com/opinions/that-didnt-last-why-m5-apple-macbook-air-is-back-to-1099-dollars>
- Collins, S. (2026, January 26). *Congress picked a fight with TikTok when it should have fixed tech policy*. Public Knowledge. Retrieved March 3, 2026, from <https://publicknowledge.org/congress-picked-a-fight-with-tiktok-when-it-should-have-fixed-tech-policy/>
- Command Linux. (2025, December 25). *Most popular Linux distributions market share 2026*. Retrieved March 3, 2026, from <https://commandlinux.com/statistics/most-popular-linux-distributions-market-share/>
- Commission Nationale de l'Informatique et des Libertés. (2025, July 11). *Caméras « augmentées » pour estimer l'âge dans les bureaux de tabac : la CNIL précise sa position*. Retrieved March 5, 2026, from <https://www.cnil.fr/fr/cameras-augmentees-pour-estimer-lage-dans-les-bureaux-de-tabac-la-cnil-precise-sa-position>
- Dawe, L. (2026, March 4). *Ubuntu and Fedora devs comment on California's new Digital Age Assurance Act*. *GamingOnLinux*. Retrieved March 4, 2026, from <https://www.gamingonlinux.com/2026/03/ubuntu-and-fedora-devs-comment-on-californias-new-digital-age-assurance-act/>
- Davis Wright Tremaine LLP. (2026, January 23). *Wave of federal 'online safety' legislation hits Congress: Federal government poised to reassert itself in the constitutionally fraught exercise of online speech regulation*. Retrieved March 3, 2026, from <https://www.dwt.com/insights/2026/01/federal-online-safety-legislation-hits-congress>

Devuan GNU+Linux. (2025). *Operating System Overview*. Retrieved March 3, 2026, from <https://www.devuan.org/os/>

Egelman, S. (2023). Informing future privacy enforcement by examining 20+ years of COPPA. *Harvard Journal of Law & Technology*, 37(3) (Symposium), 1387–1422. Retrieved March 5, 2026, from <https://jolt.law.harvard.edu/assets/articlePDFs/v37/Symposium-14-Egelman-Informing-Future-Privacy-Enforcement.pdf>

Electronic Frontier Foundation. (2025, April 29). *Age Verification in the European Union: The Commission's Age Verification App*. Retrieved March 4, 2026, from <https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet>

eSafety Commissioner. (2026, January 13). Social media age restrictions. Australian Government. Retrieved March 4, 2026, from <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>

F-Droid. (2025, August 4). Strengthening F-Droid's Legal Resilience - Introducing the Research Series. Retrieved March 4, 2026, from <https://f-droid.org/2025/08/04/strengthening-f-droids-legal-resilience-introducing-the-research-series.html>

Federal Trade Commission. (2026a). *Protection of children's privacy* (16 C.F.R. Part 312). Retrieved March 3, 2026, from <https://www.ecfr.gov/current/title-16/part-312>

Federal Trade Commission. (2026b, February 25). *FTC issues COPPA policy statement to incentivize the use of age verification technologies to protect children online*. Retrieved March 3, 2026, from <https://www.ftc.gov/news-events/news/press-releases/2026/02/ftc-issues-coppa-policy-statement-incentivize-use-age-verification-technologies-protect-children>

FOSDEM. (2026). *Age verification: A threat to the open-source ecosystem* [Conference session]. FOSDEM 2026, Brussels, Belgium. Retrieved March 3, 2026, from <https://fosdem.org/2026/schedule/event/VKYL3P-age-verification-threat-to-open-source/>

Fox Rothschild LLP. (2026, January 9). *Texas federal court enjoins Texas App Store Accountability Act on free speech grounds*. *JD Supra*. Retrieved March 5, 2026, from <https://www.jdsupra.com/legalnews/texas-federal-court-enjoins-texas-app-1860486/>

Good, T. (2025, December 9). *How much does a SOC 2 audit cost?* Workstreet. Retrieved March 5, 2026, from <https://www.workstreet.com/blog/soc-2-audit-cost>

Hogan Lovells. (2026, January 5). China announces audit reporting requirements for minors' data. JD Supra. Retrieved March 5, 2026, from <https://www.jdsupra.com/legalnews/china-announces-audit-reporting-2515590/>

James, L. (2026, March 1). *California introduces age verification law for all operating systems, including Linux and SteamOS — user age verified during OS account setup*. Tom's Hardware. Retrieved March 3, 2026, from <https://www.tomshardware.com/software/operating-systems/california-introduces-age-verification-law>

Kids Online Safety Act, S. 1748, 119th Cong. § 107 (2025). Retrieved March 3, 2026, from <https://www.congress.gov/bill/119th-congress/senate-bill/1748>

La Discussione. (2026, February 20). *Identità digitale e accesso al web: il nuovo fronte aperto dal Kids Online Safety Act*. Retrieved March 3, 2026, from <https://ladiscussione.com/421029/esteri/identita-digitale-e-accesso-al-web-il-nuovo-fronte-aperto-dal-kids-online-safety-act/>

Lima-Strong, C. (2025, December 3). Congress's bipartisan child online safety coalition is unraveling. *Tech Policy Press*. Retrieved March 3, 2026, from <https://www.techpolicy.press/congresss-bipartisan-child-online-safety-coalition-is-unraveling/>

Loeb & Loeb LLP. (2025, December). App store age verification laws trigger new federal and state children's privacy requirements. *Hashed & Salted: A Privacy and Data Security Update*. Retrieved March 3, 2026, from <https://www.loeb.com/en/insights/publications/2025/12/app-store-age-verification-laws-trigger-new-federal-and-state-childrens-privacy-requirements>

Microsoft. (2026). *Windows 11 Home (Download)* [Product page]. Microsoft Store. Retrieved March 4, 2026, from <https://www.microsoft.com/en-us/d/windows-11-home/dg7gmgf0krt0>

National Association of Attorneys General. (2025, February 10). *Supreme Court Report, Volume 32, Issue 6*. Retrieved March 3, 2026, from <https://www.naag.org/attorney-general-journal/supreme-court-report-volume-32-issue-6/>

National Law Review. (2026, March 2). *FTC releases COPPA policy statement promoting age verification technology*. Retrieved March 4, 2026, from <https://natlawreview.com/article/ftc-releases-coppa-policy-statement-promoting-age-verification-technology>

Nestor, M. (2026, March 4). Ubuntu, Fedora, Linux Mint eye age verification amid California law backlash. *9to5Linux*. Retrieved March 4, 2026, from <https://9to5linux.com/ubuntu-fedora-linux-mint-eye-age-verification-amid-california-law-backlash>

Open Source Initiative. (2026, January 26). *Open Source software, public policy, and the stakes of getting it right*. Retrieved March 3, 2026, from <https://opensource.org/blog/open-source-software-public-policy-and-the-stakes-of-getting-it-right>

Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, Div. H, 138 Stat. 895 (2024). <https://www.congress.gov/bill/118th-congress/house-bill/7521/text>

Raindog308. (2026, March 4). *Absolute insanity: Age verification for OS accounts coming to Ubuntu*. LowEndBox. <https://lowendbox.com/blog/absolute-insanity-age-verification-for-os-accounts-coming-to-ubuntu/>

Reason Foundation. (2026, January 4). *Examining California's Digital Age Assurance Act*. <https://reason.org/commentary/examining-californias-digital-age-assurance-act/>

Renew Europe. (2025, November 26). *European Parliament pushes back against Big Tech as it adopts child-safety blueprint*. <https://www.reneweuropegroup.eu/news/2025-11-26/european-parliament-pushes-back-against-big-tech-as-it-adopts-child-safety-blueprint>

Ridley, J. (2026, March 4). *Resistance to operating system age checks coming from checks notes open source calculator and an OS that may just exclude Californians altogether*. PC Gamer. <https://www.pcgamer.com/software/operating-systems/resistance-to-operating-system-age-checks-coming-from-checks-notes-open-source-calculator-and-an-os-that-may-just-exclude-californians-altogether/>

Rozenshtein, A. Z. (2025, January 20). *Trump's TikTok executive order and the limits of executive non-enforcement*. Lawfare. <https://www.lawfaremedia.org/article/trump's-tiktok-executive-order-and-the-limits-of-executive-non-enforcement>

Schneier, B. (2002). *Secrets and lies: Digital security in a networked world*. Wiley.

[Service-Public.fr](https://www.service-public.gouv.fr/particuliers/actualites/A17487?lang=en). (2024, July 11). *Parental control: new obligations for connected hardware manufacturers*. Direction de l'information légale et administrative (Premier ministre). <https://www.service-public.gouv.fr/particuliers/actualites/A17487?lang=en>

SPIRS Project. (n.d.). *Concept*. Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process. <https://www.spirs-project.eu/about-spirs/concept/>

Sridhar, A. (2025, December 18). *Regulating addictive technology for children*. The Regulatory Review. Retrieved March 4, 2026, from <https://www.theregreview.org/2025/12/18/sridhar-regulating-addictive-technology-for-children/>

StatCounter Global Stats. (2026a, January). *Desktop Operating System Market Share Worldwide*. <https://gs.statcounter.com/os-market-share/desktop/worldwide/2026>

StatCounter Global Stats. (2026c, January). *Desktop Operating System Market Share United States of America*. <https://gs.statcounter.com/os-market-share/desktop/united-states-of-america/2026>

Supreme Court of the United States. (1943). *Parker v. Brown*, 317 U.S. 341. Retrieved March 5, 2026, from <https://supreme.justia.com/cases/federal/us/317/341/>

Supreme Court of the United States. (1980). *California Retail Liquor Dealers Ass'n v. Midcal Aluminum*, 445 U.S. 97 (p. 105). Retrieved March 5, 2026, from <https://supreme.justia.com/cases/federal/us/445/97/>

Supreme Court of the United States. (1985). *Town of Hallie v. City of Eau Claire*, 471 U.S. 34. Retrieved March 5, 2026, from <https://supreme.justia.com/cases/federal/us/471/34/>

Suzuki, T. (2024). Self-Sovereign Identity with Sybil-resistance using Attested Execution Secure Processors. *Journal of Information Processing*, 32, 456-468. <https://doi.org/10.2197/ipsjip.32.456>

TikTok Inc. v. Garland, No. 24-656, 604 U.S. ____ (2025). https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf

This report is based on analysis of California AB 1043, Colorado SB 26 051, Texas SB 2420, Utah's and Louisiana's App Store Accountability Acts, the Kids Online Safety Act (S. 1748) as introduced in the 119th Congress, 16 CFR Part 312 as updated through March 2, 2026, constitutional law principles, open source software dynamics, international jurisdiction frameworks, European Union privacy law, and the sources cited above. It represents a comprehensive examination of the coordinated state federal regulatory framework, its provisions, implications, and the deeper structural concerns raised by critical analysis.

Prepared for educational and advocacy purposes. Not legal advice.

DeepSeek AI was used as a tool to assist with the organization, citation formatting, compiling and preliminary conceptual development of this draft. This acknowledgement is for full transparency and reference only.